



Booking for Outlook Setup Guide



Setting up Room Resource Account and SharePoint

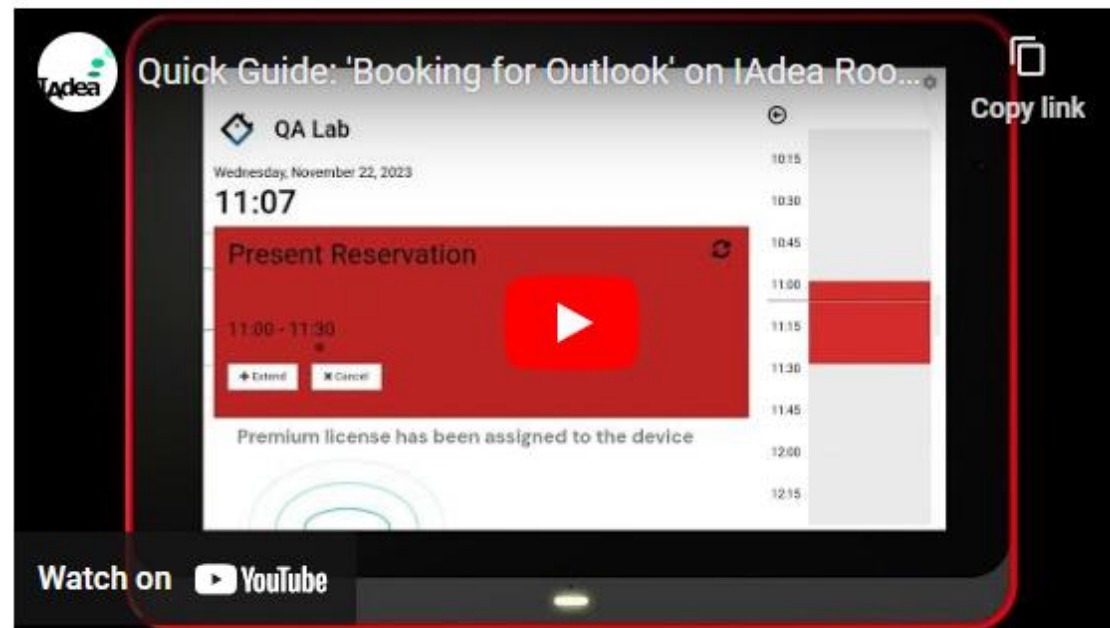
By: IAdea FAE

08/01/2025

Booking for Outlook Tutorial – The Introduction

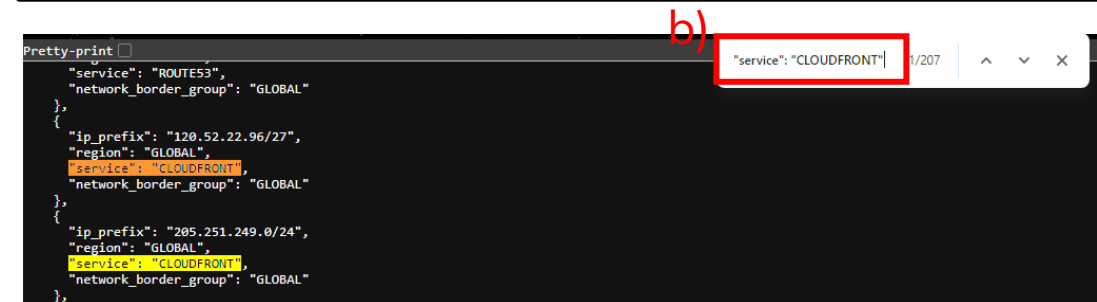
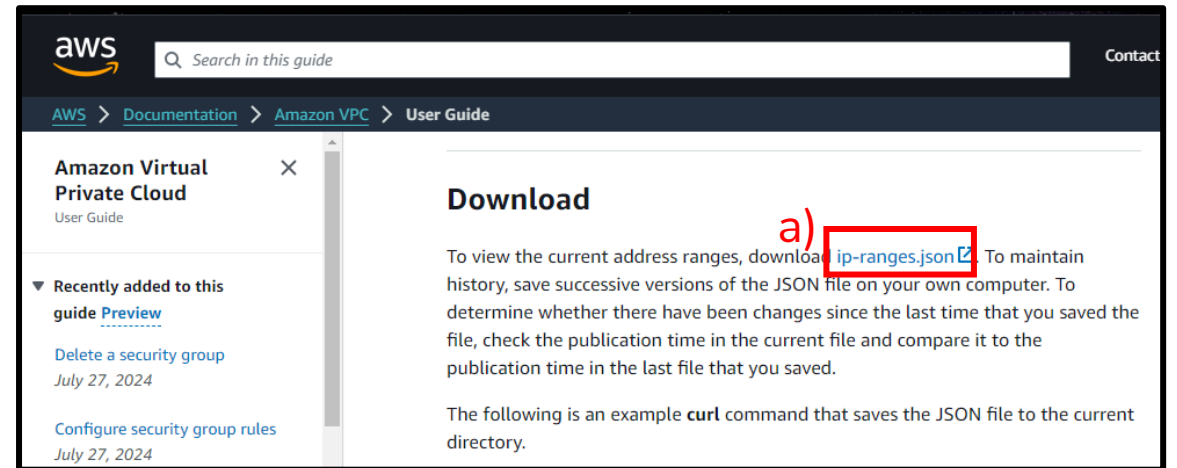
- <https://support.iadea.com/hc/en-us/articles/25874019540761-Booking-For-Outlook-Tutorial-The-Introduction>

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



List of IPs and Domains to Whitelist

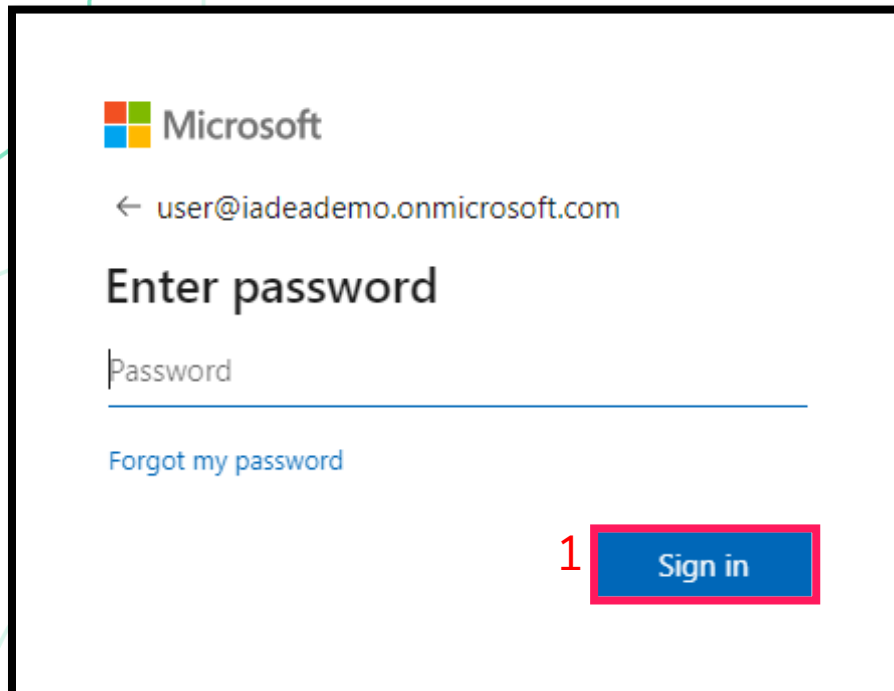
- Please allow both the domain and IP to minimize any network issues:
1. Responsible for license and API: <https://support.iadea.com/hc/en-us/articles/360001155223-IdeaCare-Why-is-my-device-not-receiving-a-pairing-code-or-always-showing-offline-on-the-IdeaCare-website>
 2. Responsible for UI (AWS and 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](#)



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.



Microsoft

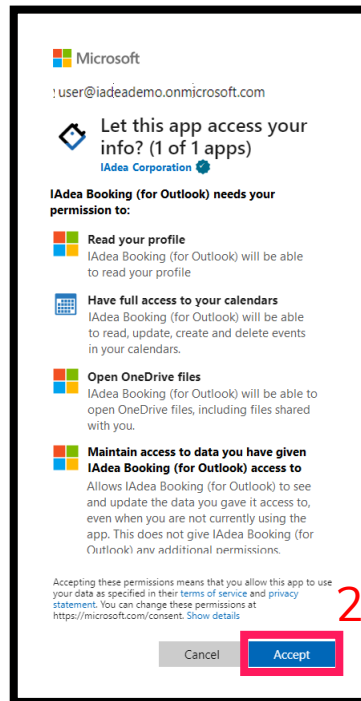
← user@iadeademo.onmicrosoft.com

Enter password

Password

[Forgot my password](#)

1 [Sign in](#)



Microsoft

user@iadeademo.onmicrosoft.com

Let this app access your info? (1 of 1 apps)

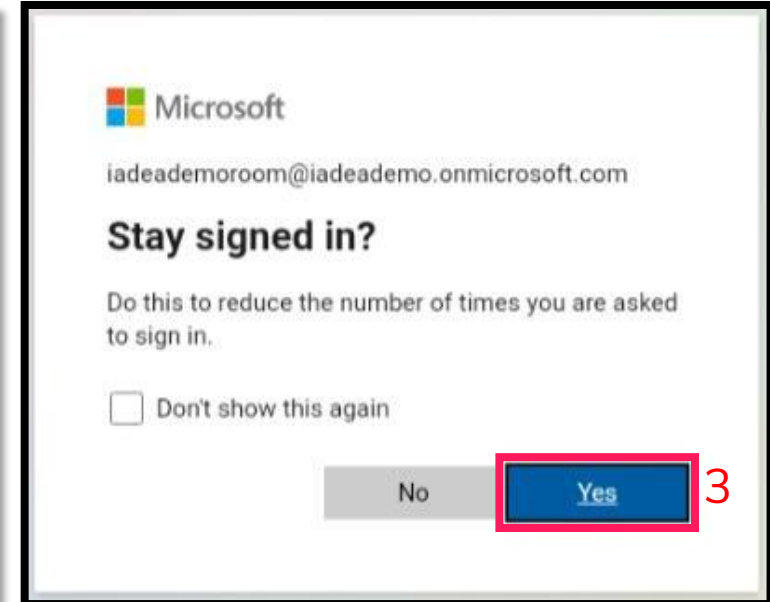
Idea Corporation

Idea Booking (for Outlook) needs your permission to:

- Read your profile**
Idea Booking (for Outlook) will be able to read your profile.
- Have full access to your calendars**
Idea Booking (for Outlook) will be able to read, update, create and delete events in your calendars.
- Open OneDrive files**
Idea Booking (for Outlook) will be able to open OneDrive files, including files shared with you.
- Maintain access to data you have given Idea Booking (for Outlook) access to**
Allows Idea Booking (for Outlook) to see and update the data you gave it access to, even when you are not currently using the app. This does not give Idea Booking (for Outlook) any additional permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at <https://microsoft.com/consent>. [Show details](#)

[Cancel](#) [Accept](#) 2



Microsoft

iadeademoroom@iadeademo.onmicrosoft.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

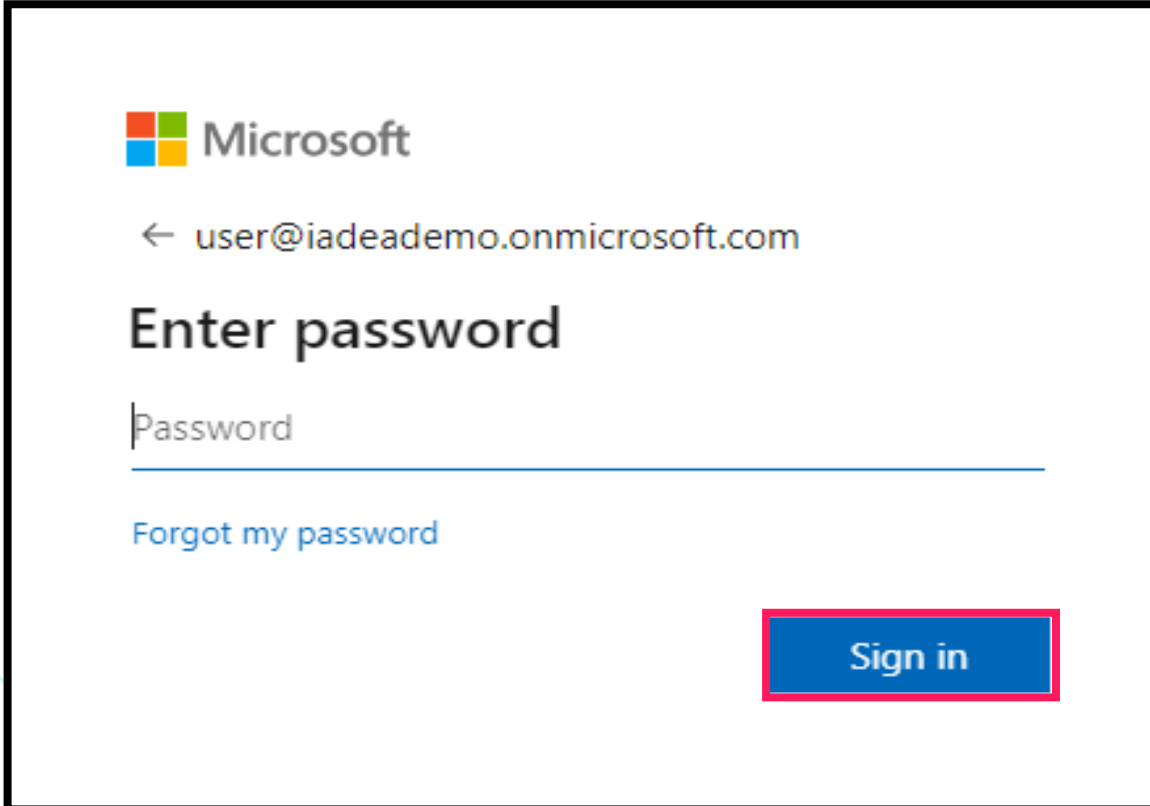
[No](#) [Yes](#) 3

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/>.

A screenshot of the Microsoft Office 365 Admin Portal login page. The page features the Microsoft logo at the top left. Below it, there is a back arrow and the email address 'user@iadeademo.onmicrosoft.com'. The main heading is 'Enter password'. Below this is a password input field with the placeholder text 'Password'. Under the input field is a link that says 'Forgot my password'. At the bottom right, there is a blue 'Sign in' button with a red border.

Microsoft

← user@iadeademo.onmicrosoft.com

Enter password

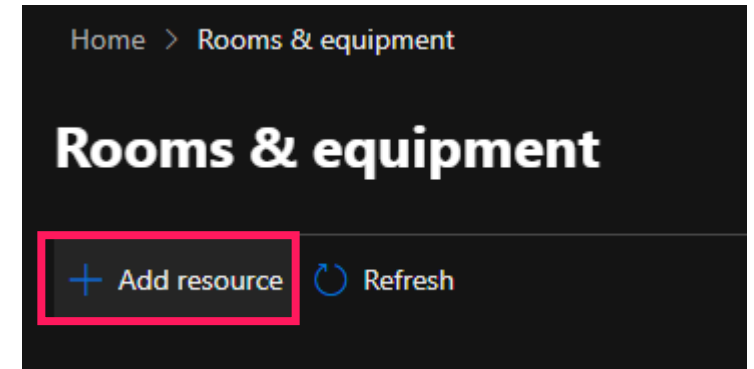
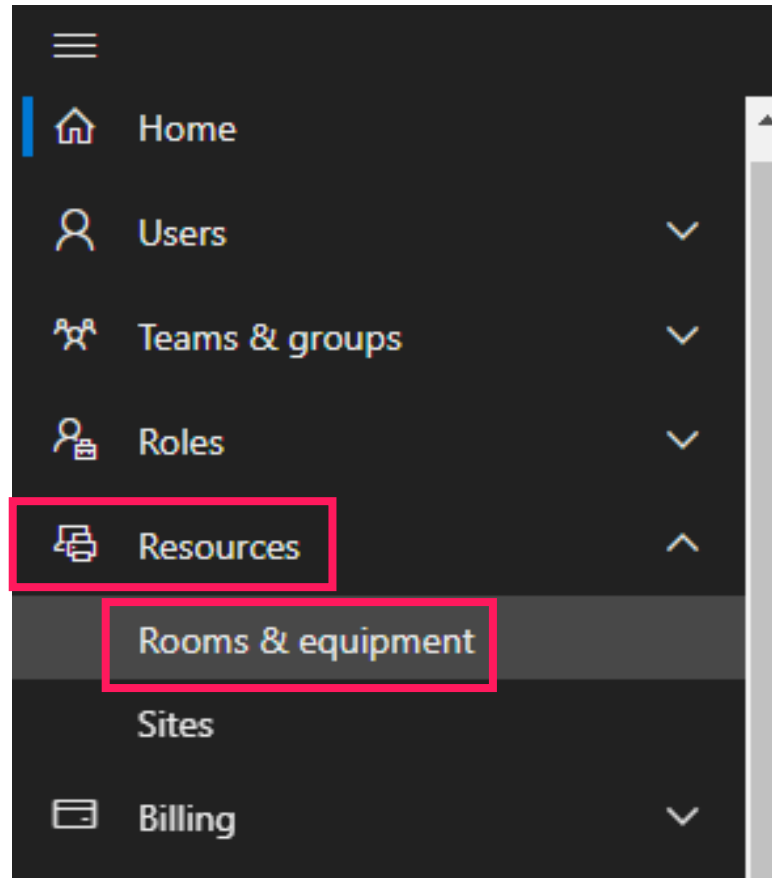
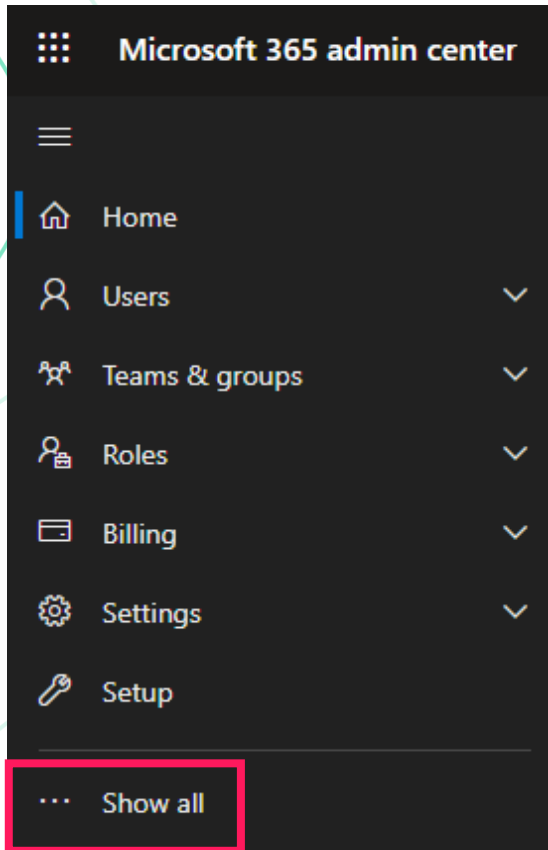
Password

[Forgot my password](#)

Sign in

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].

Add resource

Create a mailbox for things like a conference room, company car, or equipment that everyone needs to use, so that those resources are reservable.

[Learn more about resource types](#)

Resource type

Room

Name *

IAdeaDemoRoom

The resource name appears in the address book, and in the To and From lines in meeting invitations and responses.

Email *

IAdeaDemoRoom

@

Domains

iadeademo.onmicrosoft.com

The email address is used to send meeting invitations to the resource.

Capacity

4

The number of people who can fit in the room or use the equipment at the same time.

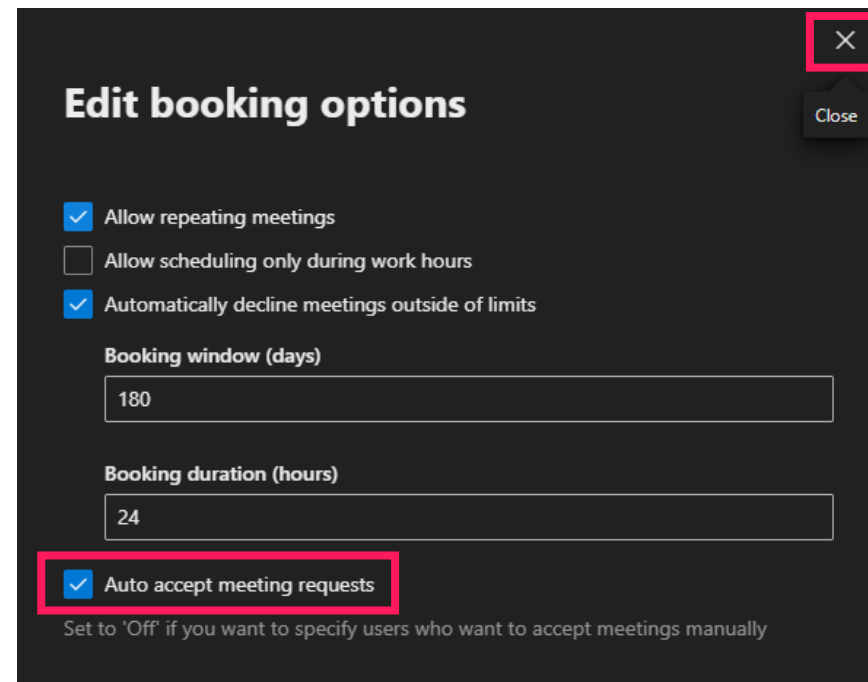
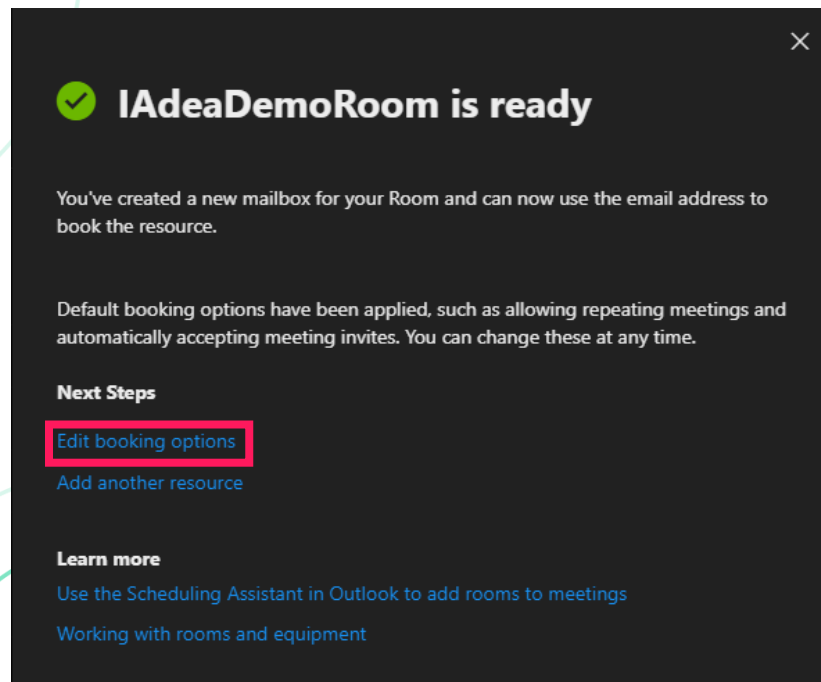
Location

Phone number

Save

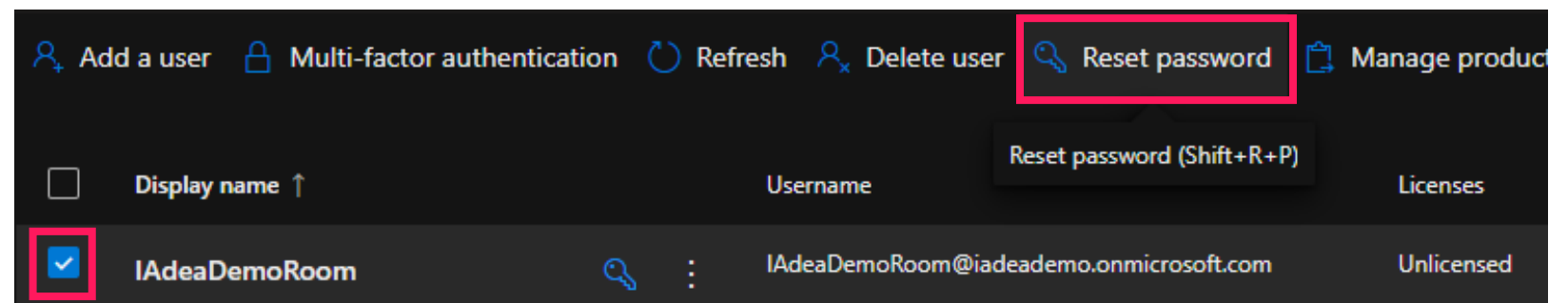
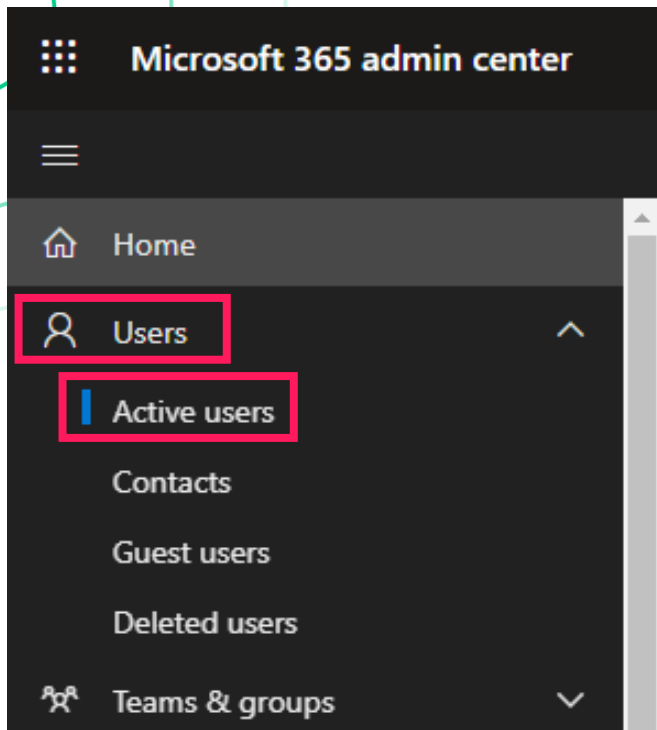
4. Adjusting Booking Preferences

- 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].

Reset password

IAdeaDemoRoom@iadeademo.onmicrosoft.com

☒ Automatically create a password

Passwords must be between 8 and 256 characters and use a combination of at least three of the following: uppercase letters, lowercase letters, numbers, and symbols.

Password *

.....

Strong

☐ Require this user to change their password when they first sign in

☒ Email the sign-in info to me

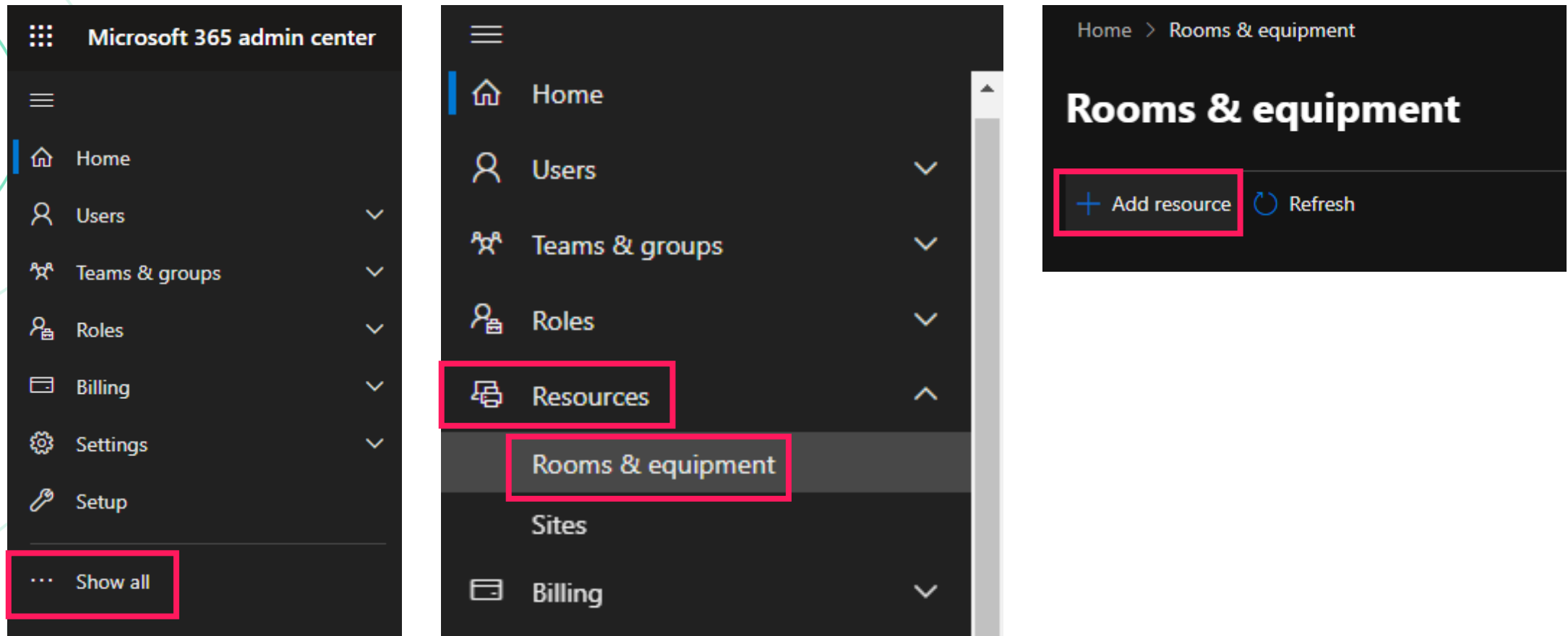
Your email *

user@iadeademo.onmicrosoft.com

Reset password

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.

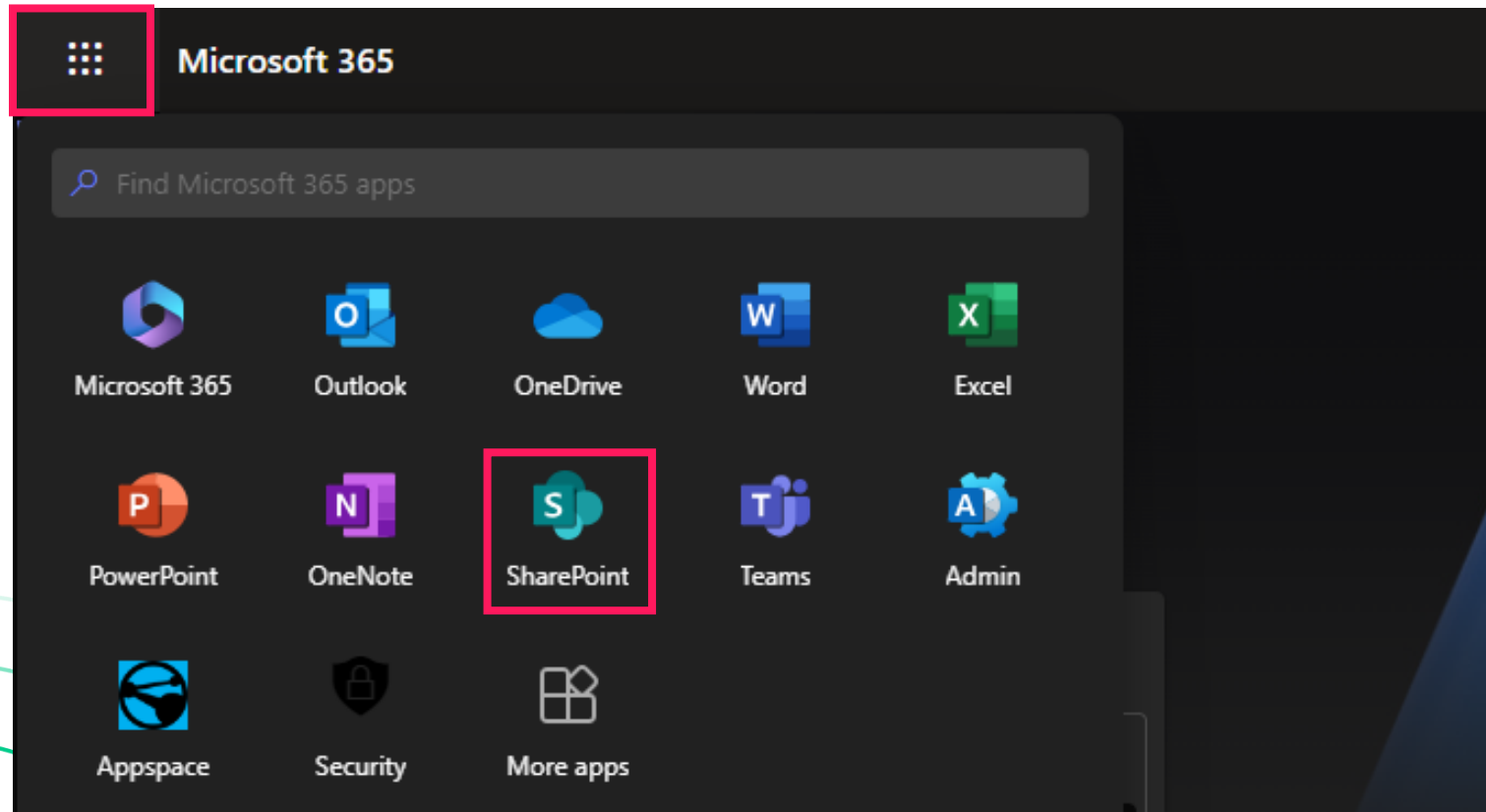


Step 2. Identifying the SharePoint Root Site

- Access SharePoint through Office365
 - Identify the Root Site

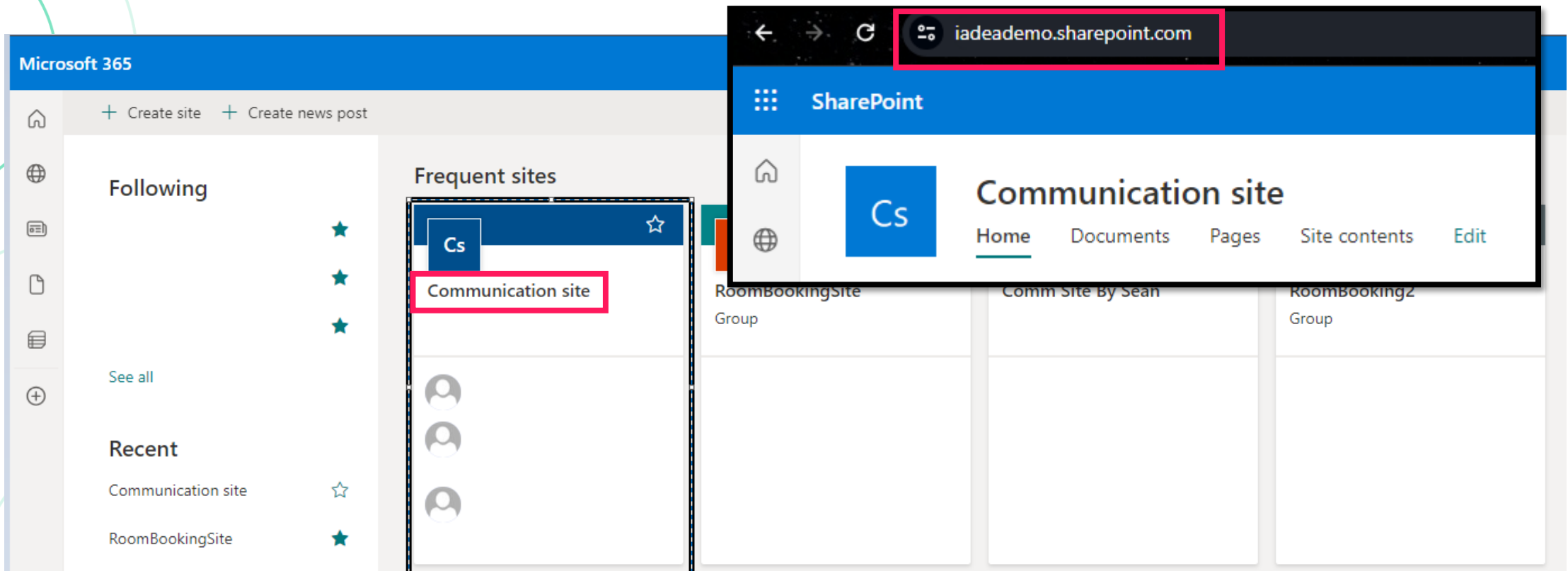
1. Accessing Office365 and Launching SharePoint

- 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].sharepoint.com'.

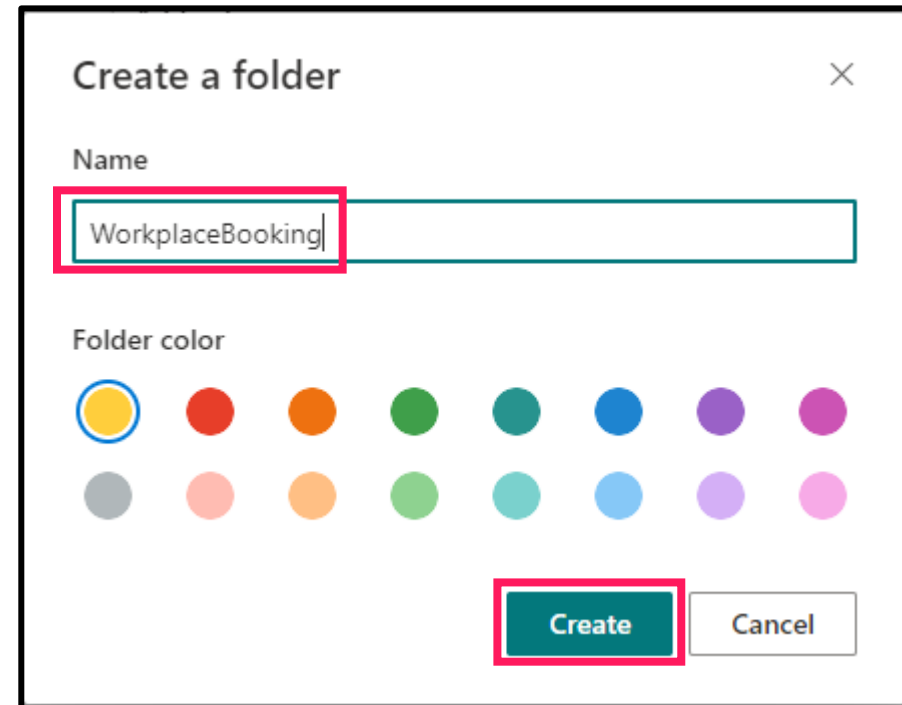
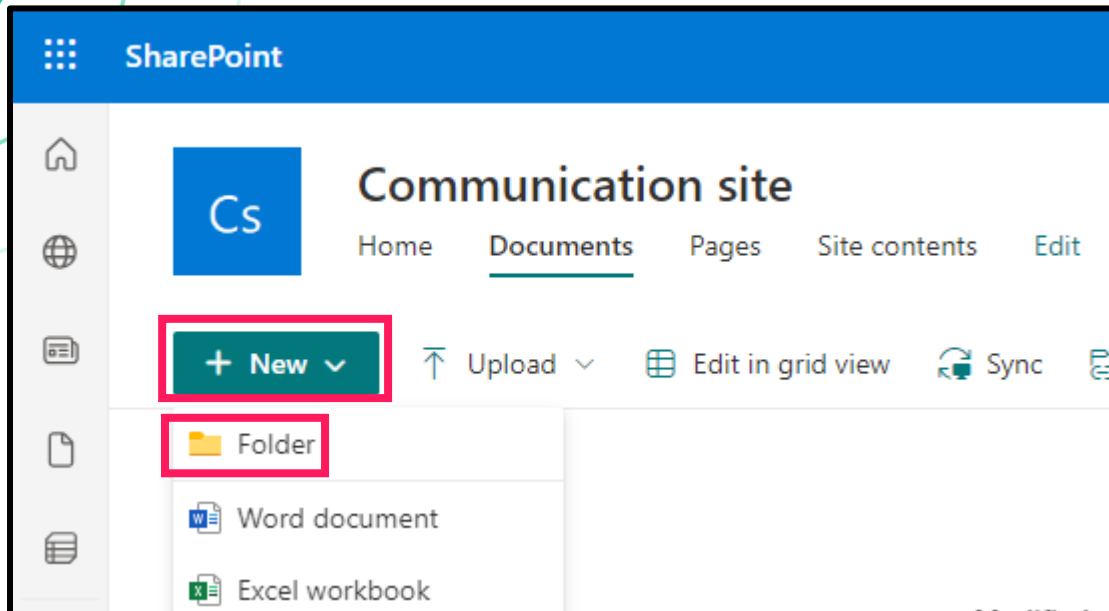


Step 3. Configuring Files on SharePoint

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

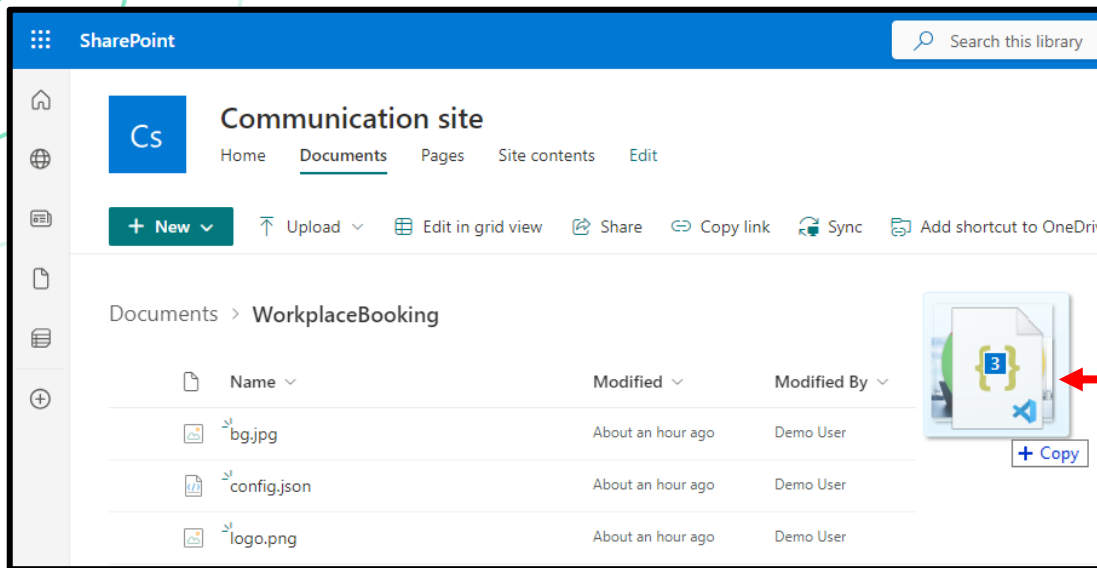
1. Creating a New Folder Named WorkplaceBooking

- 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

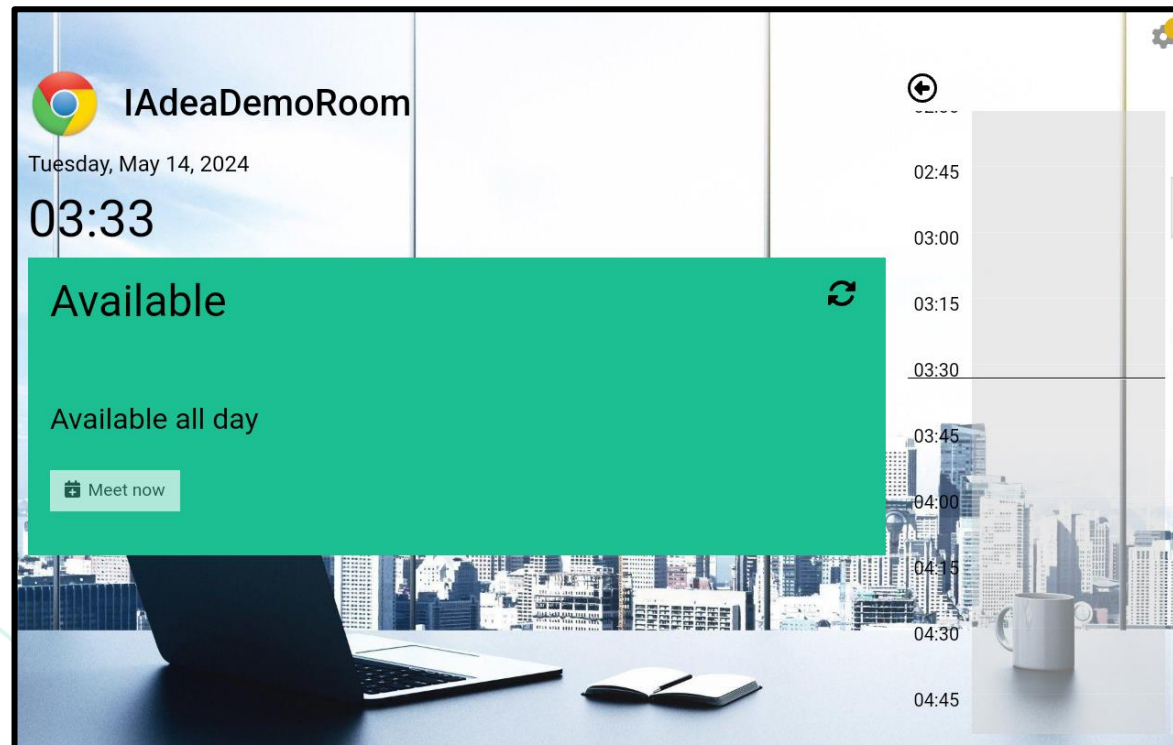
- Choose a background picture and your company's logo for Booking for Outlook (Name it bg.jpg and logo.png).
- Drag the selected files along with the config.json provided and paste them into the WorkplaceBooking folder.



BookingForOutlook				
Name	Date modified	Type	Size	
bg.jpg	5/13/2024 3:20 PM	JPG File	240 KB	
config.json	5/13/2024 3:17 PM	JSON Source File	1 KB	
logo.png	5/13/2024 3:20 PM	PNG File	120 KB	

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"
    }
  }
}
```

Setup Checks → Common Fixes

1. Resources not showing → Graph permissions
2. Keeps logging out → Organization policies
3. Text shows lang.* → Language files blocked
4. License not retrieved → Network allowlist/ firewall
5. UI broken (white/black screen) → Network allowlist/ firewall

1. Resources Data Is Not Displayed Properly

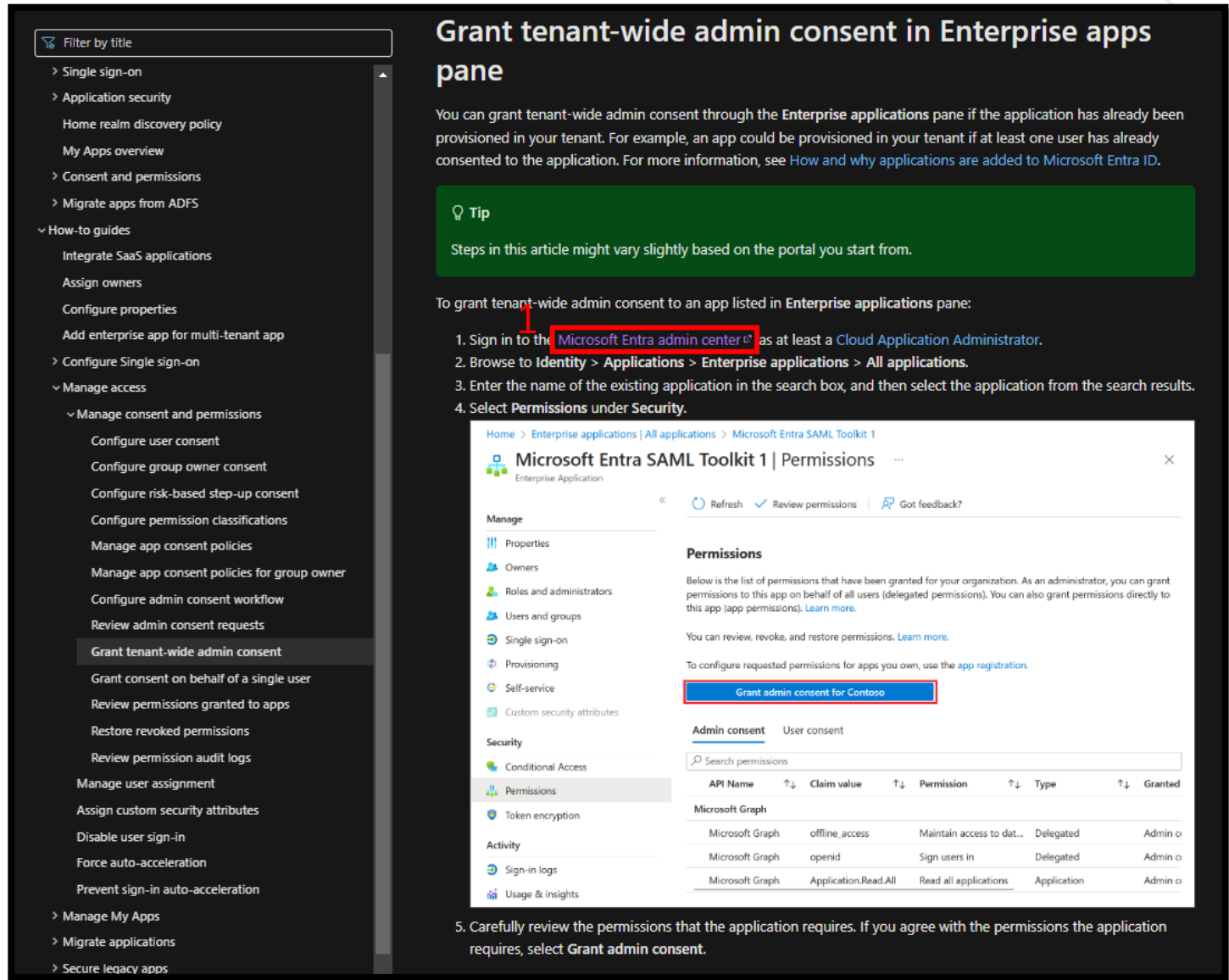
Note: If the first sign-in was Global Admin, consent is granted automatically. If not, have a Global Admin sign in once or grant admin consent.

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

- **Fix:** Manually Grant App Access

1. Follow this link for detailed instructions:

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent?pivot=portal>



Grant tenant-wide admin consent in Enterprise apps pane

You can grant tenant-wide admin consent through the Enterprise applications pane if the application has already been provisioned in your tenant. For example, an app could be provisioned in your tenant if at least one user has already consented to the application. For more information, see [How and why applications are added to Microsoft Entra ID](#).

Tip

Steps in this article might vary slightly based on the portal you start from.

To grant tenant-wide admin consent to an app listed in Enterprise applications pane:

1. Sign in to the **Microsoft Entra admin center** as at least a Cloud Application Administrator.
2. Browse to **Identity > Applications > Enterprise applications > All applications**.
3. Enter the name of the existing application in the search box, and then select the application from the search results.
4. Select **Permissions under Security**.

Home > Enterprise applications | All applications > Microsoft Entra SAML Toolkit 1

Microsoft Entra SAML Toolkit 1 | Permissions

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Self-service
- Custom security attributes

Security

- Conditional Access
- Permissions**
- Token encryption

Activity

- Sign-in logs
- Usage & insights

Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). [Learn more](#).

You can review, revoke, and restore permissions. [Learn more](#).

To configure requested permissions for apps you own, use the [app registration](#).

Grant admin consent for Contoso

Admin consent | User consent

Search permissions

API Name	Claim value	Permission	Type	Granted
Microsoft Graph				
Microsoft Graph	offline_access	Maintain access to dat...	Delegated	Admin c...
Microsoft Graph	openid	Sign users in	Delegated	Admin c...
Microsoft Graph	Application.Read.All	Read all applications	Application	Admin c...

5. Carefully review the permissions that the application requires. If you agree with the permissions the application requires, select **Grant admin consent**.

1. Resources Data Is Not Displayed Properly

Note: If the first sign-in was Global Admin, consent is granted automatically. If not, have a Global Admin sign in once or grant admin consent.

- **Symptoms:** Consistency and reliability problems; some data is either not updating correctly or disappearing.
- **Fix:** Manually Grant App Access
 2. Verify that all claim values are listed under [Admin consent].
 3. If not, click [Grant admin consent]
 4. Log in and click [Accept]

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation options like 'Diagnose & solve problems', 'Favorites', 'Identity', 'Overview', 'Users', 'Groups', 'Devices', 'Applications', 'Roles & admins', 'Protection', 'Identity Governance', and 'External Identities'. The main content area is titled 'IAdea Booking (for Outlook) | Permissions'. It includes a 'Permissions' section with a table of granted permissions. A red box labeled '2' highlights the 'User.Read' permission. Another red box labeled '3' highlights the 'Grant admin consent for IAdea America Corp.' button. A third red box labeled '4' highlights the 'Accept' button in the consent dialog.

API name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph (7)					
Microsoft Graph		User.Read	Sign in and read user profile		
Microsoft Graph		Calendars.ReadWrite	Have full access to user calendars		
Microsoft Graph		Files.Read.All	Read all files that user can access		
Microsoft Graph		Sites.Read.All	Read items in all site collections		
Microsoft Graph		openid	Sign users in		
Microsoft Graph		profile	View users' basic profile		
Microsoft Graph		offline_access	Maintain access to data you have given it access		

Microsoft
user@iadeademo.onmicrosoft.com
Permissions requested
Review for your organization
IAdea Booking (for Outlook)
Adea Corporation
This app would like to:
✓ Sign in and read user profile
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)
Does this app look suspicious? [Report it here](#)
Cancel Accept

2. Account Keeps Logging Out

- **Issue:** Booking for Outlook device prompts for login after a set period.
- **Reference on MS Teams Rooms Limitation:** <https://learn.microsoft.com/en-us/microsoftteams/troubleshoot/teams-rooms-and-devices/teams-rooms-resource-account-sign-in-issues>
 - *Notes: Do not follow the instructions blindly, as Booking for Outlook and MS Teams Rooms are separate apps (reference purpose only).*
- **Solutions for Frequent Sign-In Request Issues:**
 - a) **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](#)
 - b) **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](#)
 - c) **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.

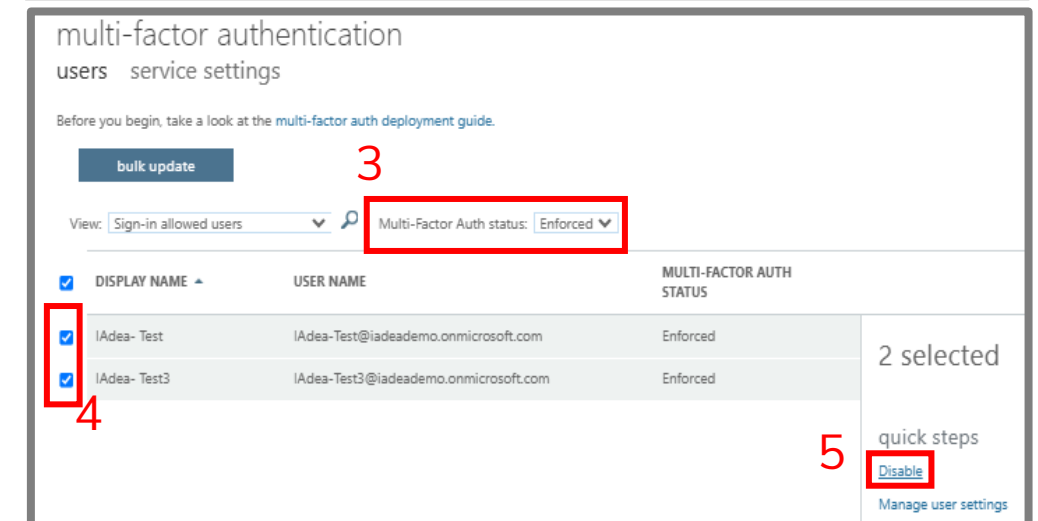
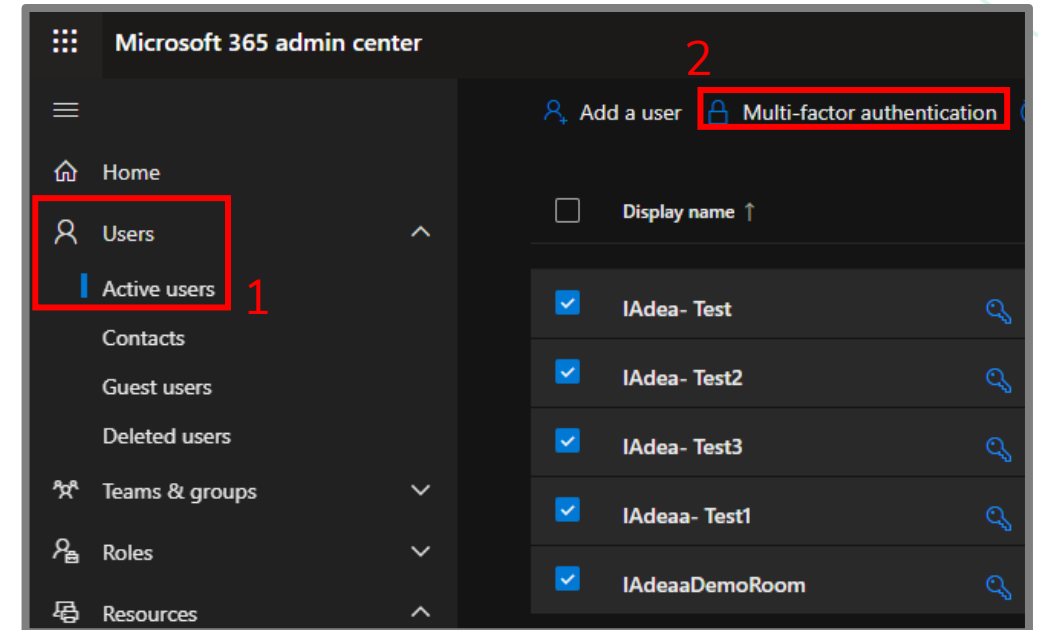
a. Disable Per-User MFA in MS365 Admin Center

- **Symptoms:** 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**.



b. Disable CAP for [IAdea Booking (for Outlook)] in Microsoft Entra Admin Center.

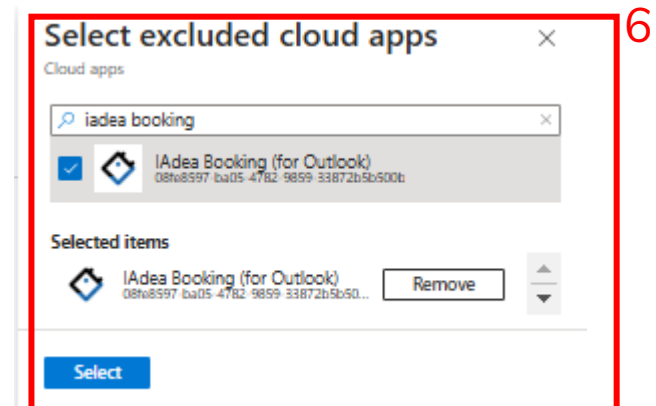
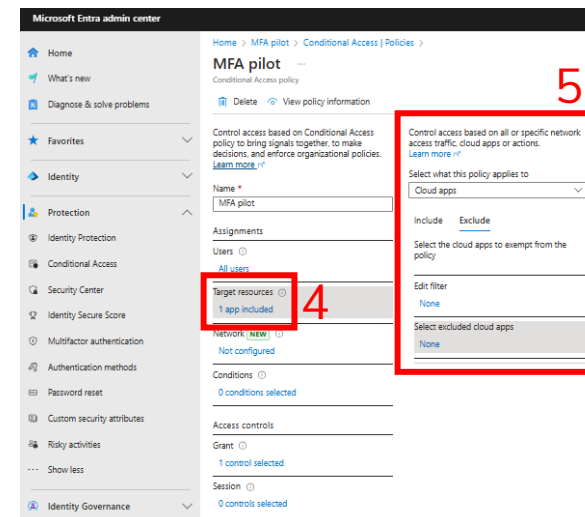
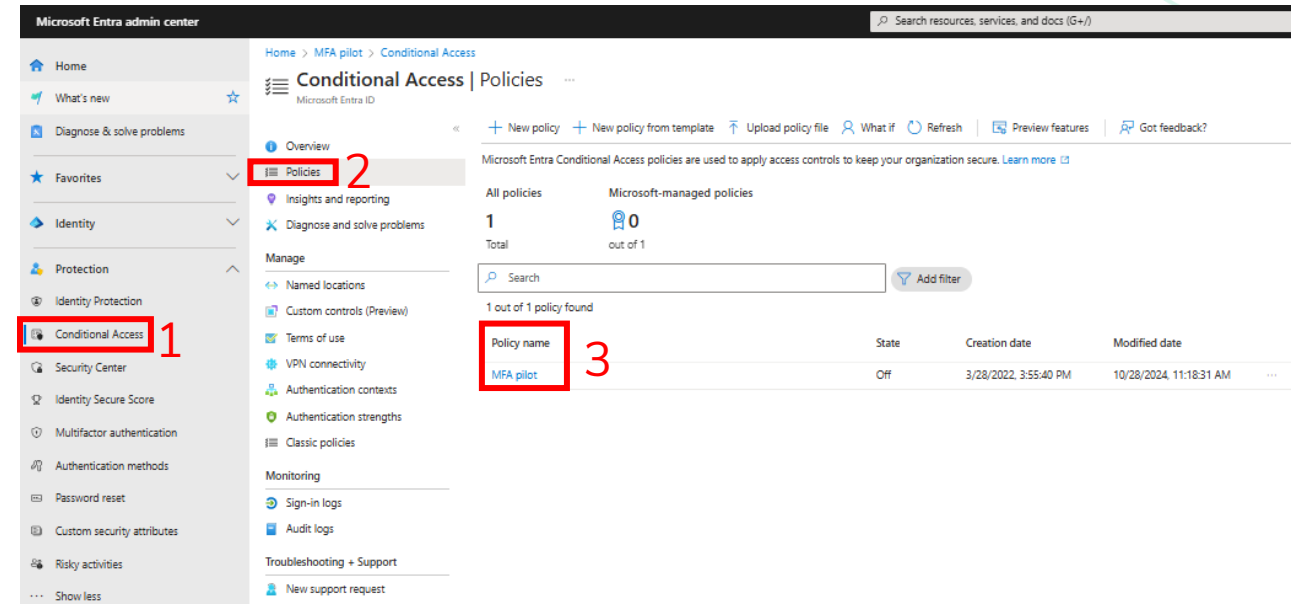
- **Symptoms:** Booking for Outlook device prompts for login after a set period.

- **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](#)



c. Disable Password Expiration for Resource Account

- **Symptoms:** Booking for Outlook device prompts for login after a set period.
- **Fix:**
 1. **Microsoft Graph PowerShell or AD (On-premises)** is required to disable password expiration for specific accounts.
 2. **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](#)

To turn off password expiration, follow the steps in one of the following tabs:

Microsoft Graph PowerShell

Active Directory (On-premises)

1. Connect to **Microsoft Graph PowerShell**:

PowerShell

Copy

```
Connect-MgGraph -Scopes "User.ReadWrite.All"
```
2. Set the password to never expire, this example sets the password for the account ConferenceRoom01@contoso.com to never expire.

PowerShell

Copy

```
Update-MgUser -UserId ConferenceRoom01@contoso.com -PasswordPolicies DisablePasswordExpiration -Pas
```

To turn off password expiration, follow the steps in one of the following tabs:

Microsoft Graph PowerShell

Active Directory (On-premises)

1. Connect to **Active Directory PowerShell**:

PowerShell

Copy

```
Import-Module ActiveDirectory
```
2. Set the password to never expire, this example sets the password for the account ConferenceRoom01@contoso.com to never expire.

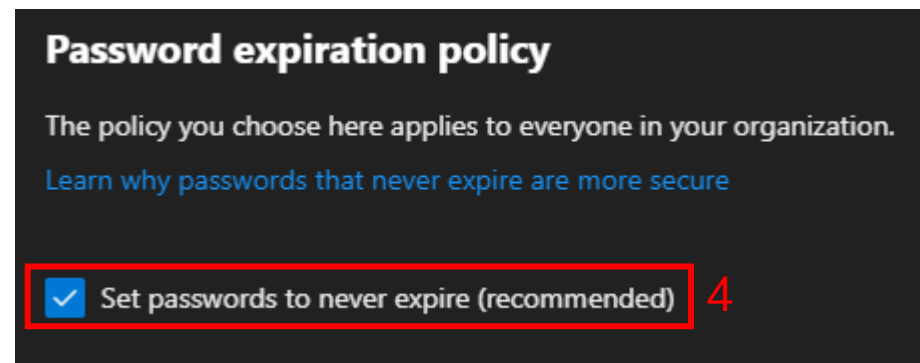
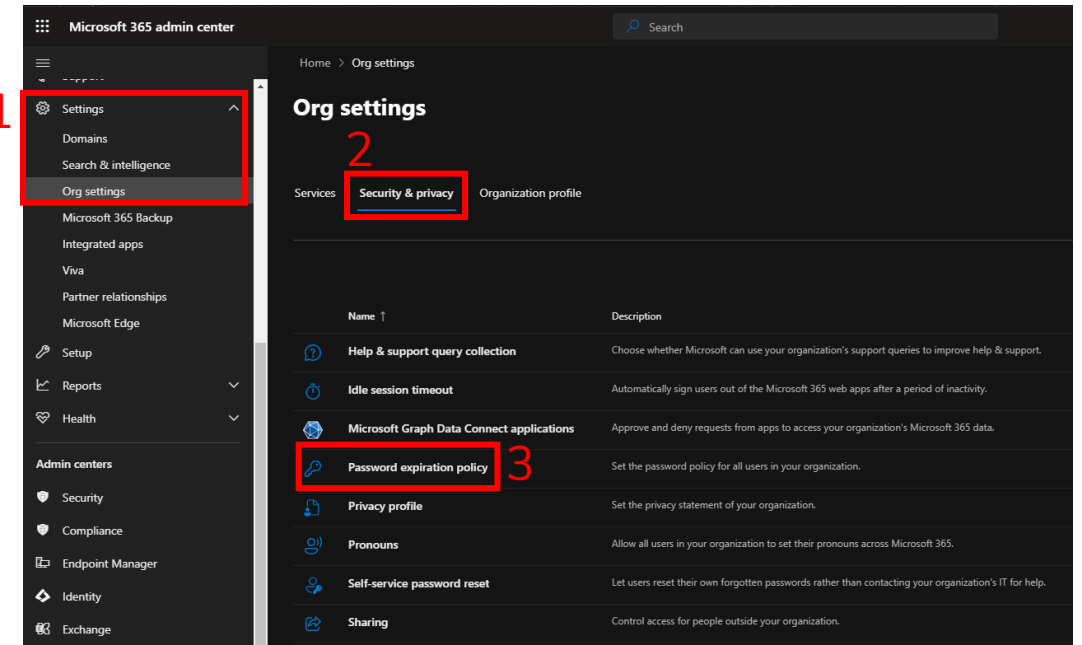
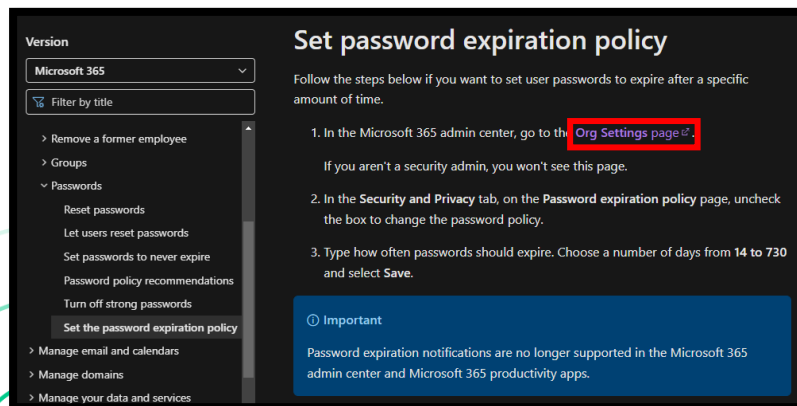
PowerShell

Copy

```
Set-ADUser -Identity ConferenceRoom01@contoso.com -PasswordNeverExpires $true
```

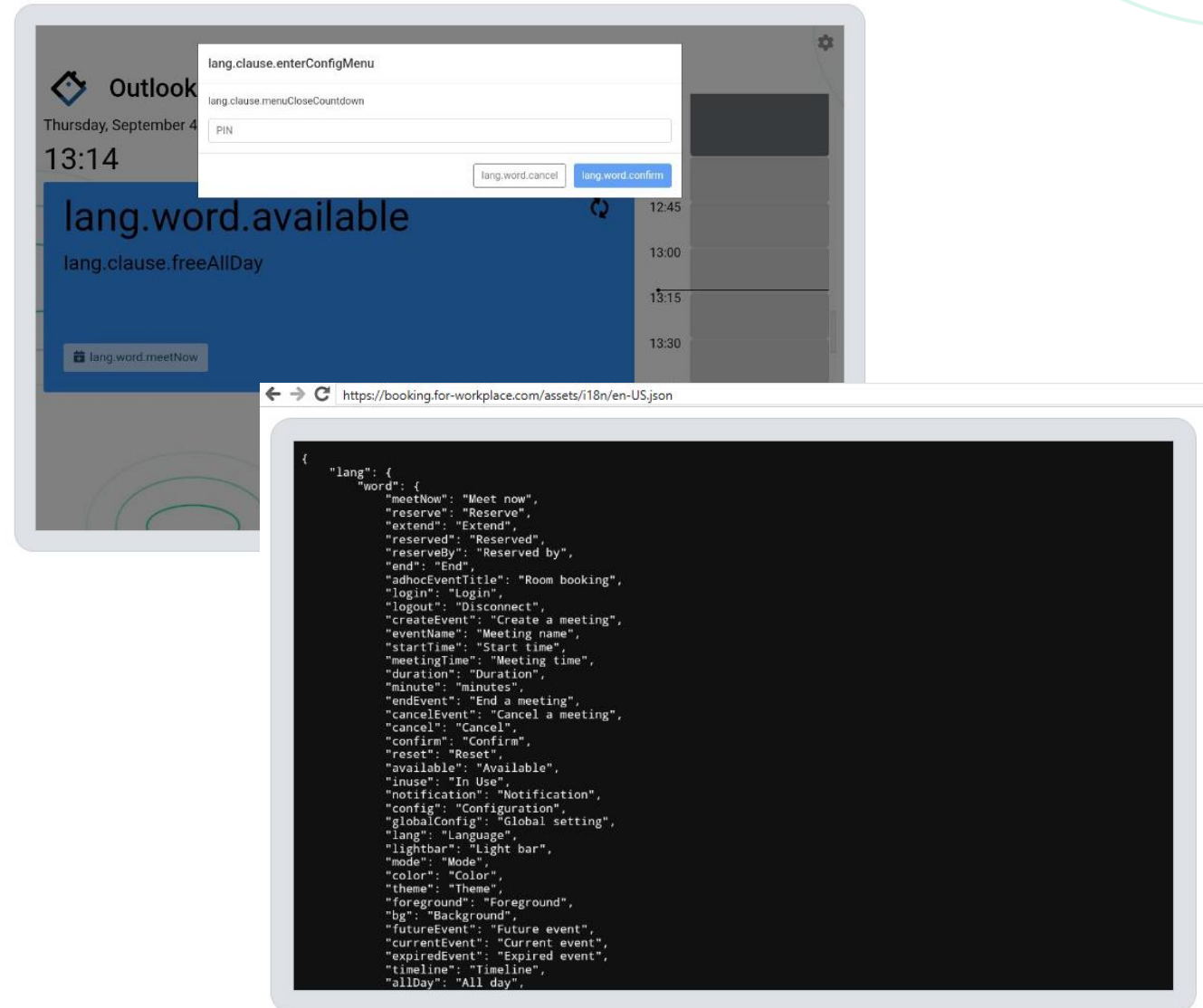
c. Disable Password Expiration on MS365 Admin Center (Alternative)

- **Symptoms:** 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. UI Text Shows lang.*

- **Symptoms:** Button/labels display keys like lang.word.extend or similar. This happens when the browser can't load the language file (e.g., en-US.json).
- **Fix: Allow language file in the network**
 1. Verify file access: In the browser, open <https://booking.for-workplace.com/assets/i18n/en-US.json>
 2. Ask IT to allow it: Request access to the webpage.



4. Unable to Retrieve License Information

- **Symptoms:** Buttons are still greyed out even when license has been activated (check notification to confirm).
- **Fix: Allowlist/ firewall/ proxy check**
 1. Allowlist: <https://support.iadea.com/hc/en-us/articles/360001155223-IdeaCare-Why-is-my-device-not-receiving-a-pairing-code-or-always-showing-offline-on-the-IdeaCare-website> (Responsible for license and API)

IdeaCare - Why is my device not receiving a pairing code or always showing offline on the IdeaCare website?

ON THIS PAGE

IdeaCare - Why is my device not...

If you cannot get the pairing code properly or the device is always showing offline on IdeaCare website, please follow the instructions below.

Step 1.

Confirm that your network environment allows HTTPS.

If you have confirmed that the network supports HTTPS but the issue persists, please proceed to step 2.

Step 2.

Ensure that the following domain names are accessible through your firewall and DNS (Domain Name Server) settings:

- api.iadea.com
- api.iadea.oniadea.com
- files.iadea.oniadea.com
- remote.iadea.oniadea.com

If reaching the DNS is impossible, please manually add the four IdeaCare current server IPs of IdeaCare to your firewall exception list:

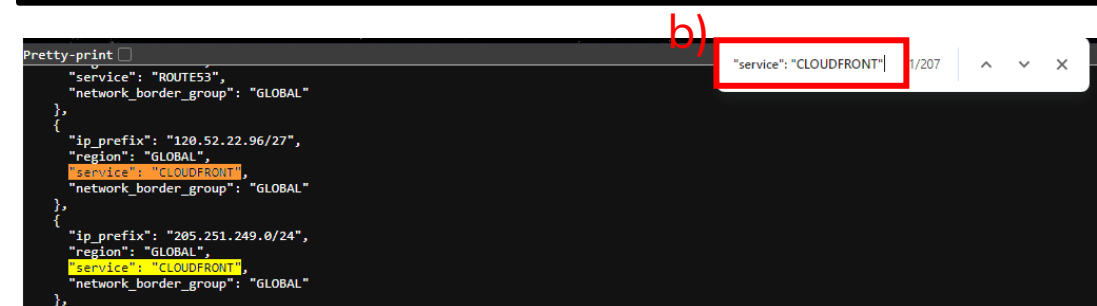
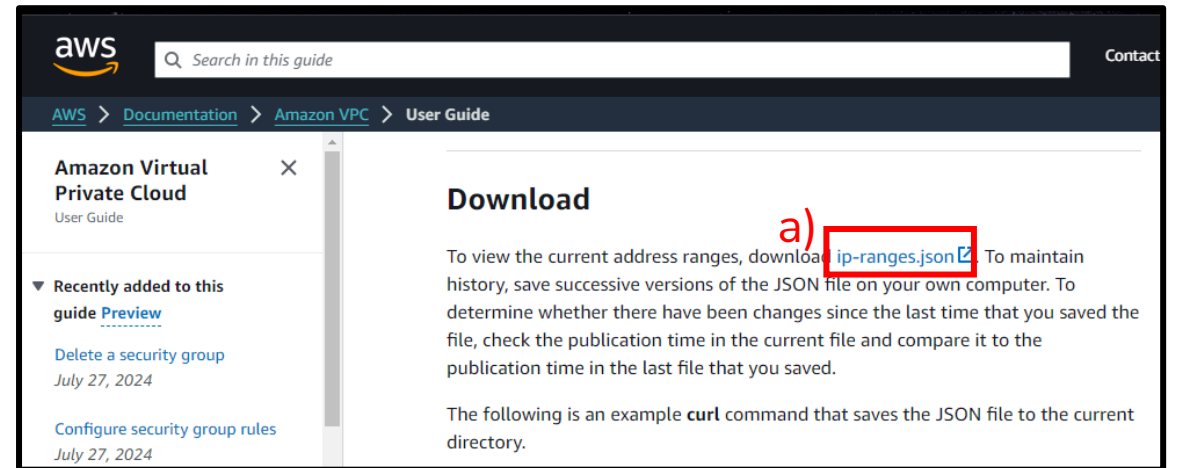
- 100.20.226.90
- 100.20.103.117
- 54.69.157.24
- 34.223.189.82
- 35.167.4.211
- 54.68.244.9
- 52.24.182.232
- 44.238.81.234
- 44.235.242.193

If the device is stuck on Initializing

Please refer to the [Initializing Article](#).

5. Broken UI/ Black Screen/ White Screen

- **Symptoms:** Device keeps rebooting, black screen, white screen, UI is broken.
- **Fix: Allowlist/ firewall/ proxy check**
 1. Test using mobile hotspot.
 2. Load URL from Chrome's app from the Android home page to see what error message being returned.
 3. Allowlist:
<https://docs.aws.amazon.com/vpc/latest/userguide/aws-ip-ranges.html> (Responsible for UI: AWS and CloudFront)
 - 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.
 4. Allowlist: [office365/Azure/AD](#) (Responsible for UI: AWS and CloudFront)
 5. Allowlist: [booking.for-workplace.com](#) (Domain)





Thank you

America

20 Fairbanks, Suite 170
Irvine, CA 92618
USA

Contact Us

Product questions

Sales@IAdea.com

Technical Assistance

Support@IAdea.com

Taiwan

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