



Booking for Outlook Setup Guide



Setting up Room Resource Account and SharePoint

By: IAdea FAE

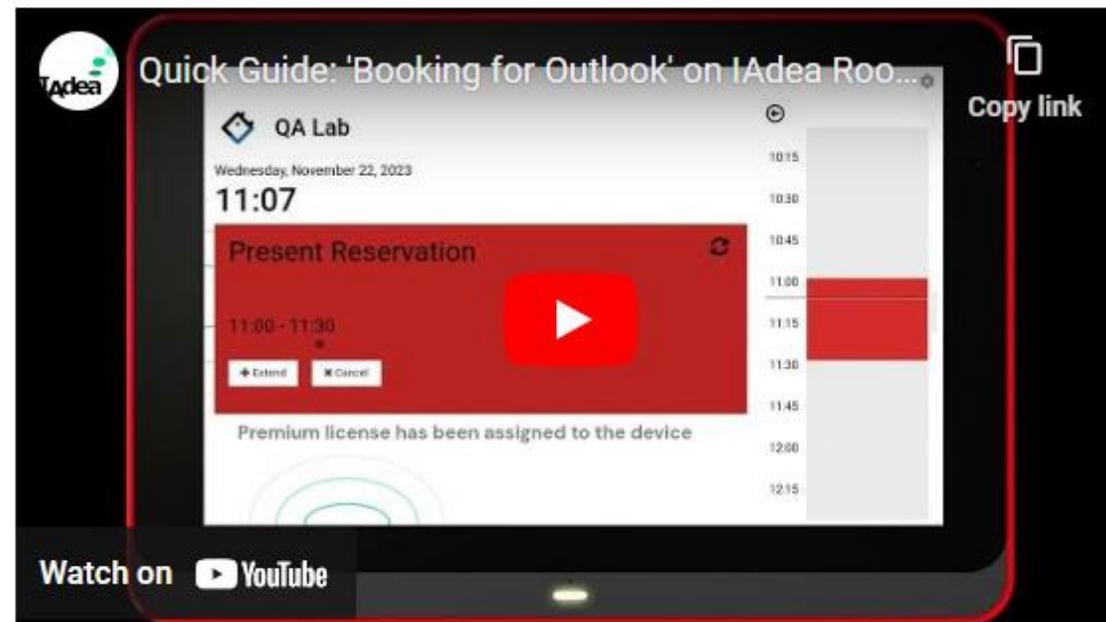
8/21/2024



Booking for Outlook Tutorial – The Introduction

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

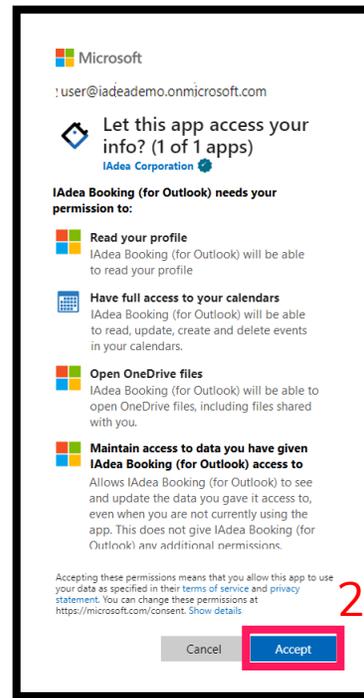
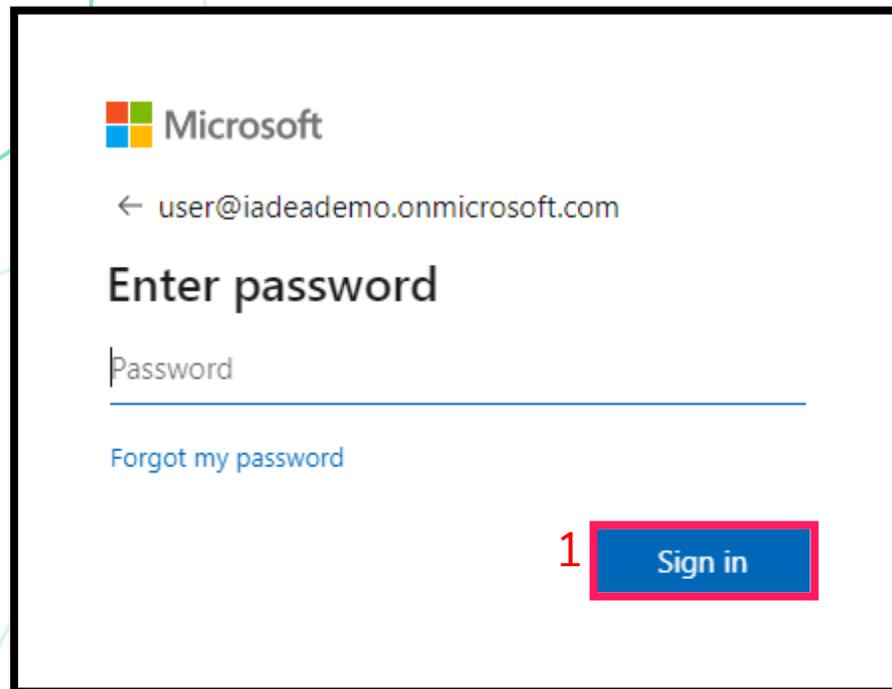
A comprehensive overview of the introductory video, guiding you through the initial setup and key features of Booking for Outlook:



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.

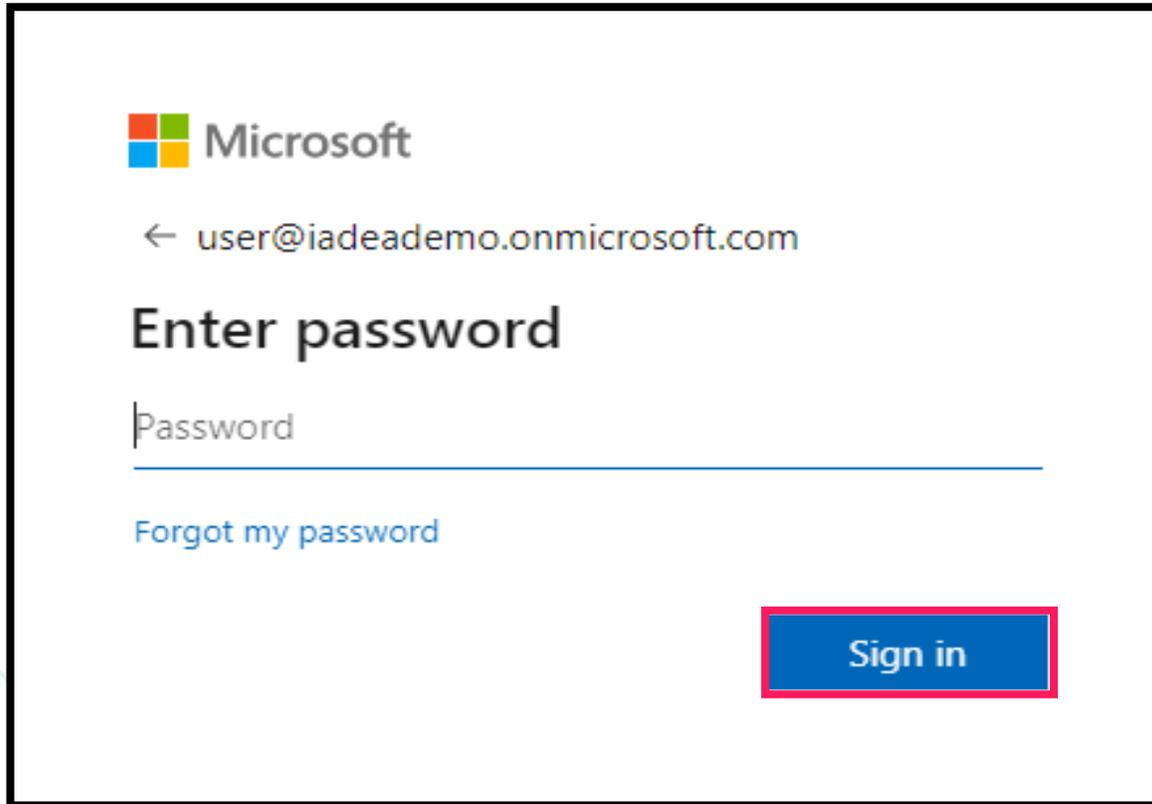


Step 1. Creating Room Resource Account

- 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/>.



Microsoft

← user@iadeademo.onmicrosoft.com

Enter password

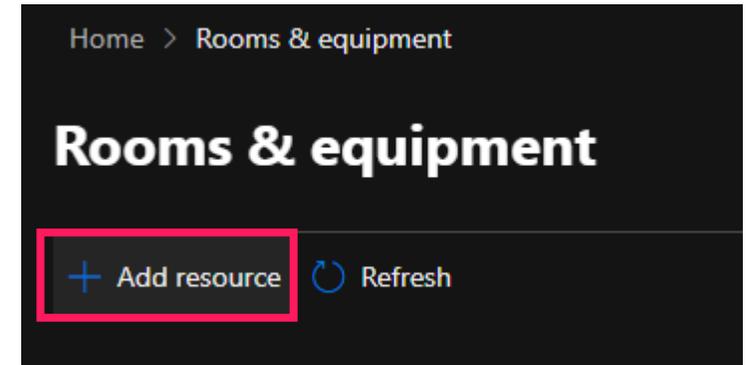
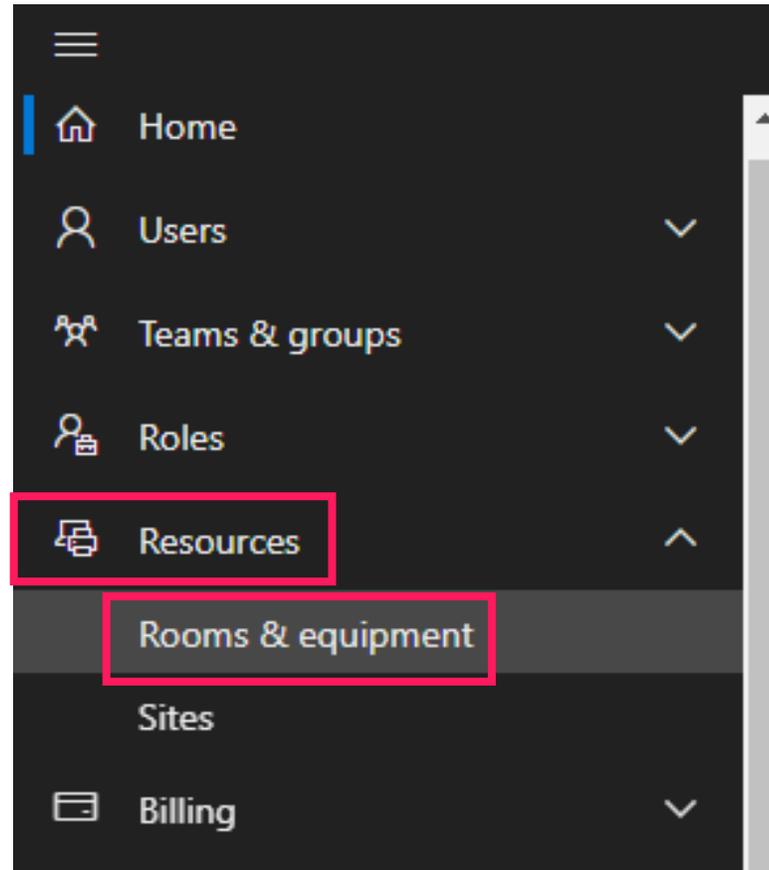
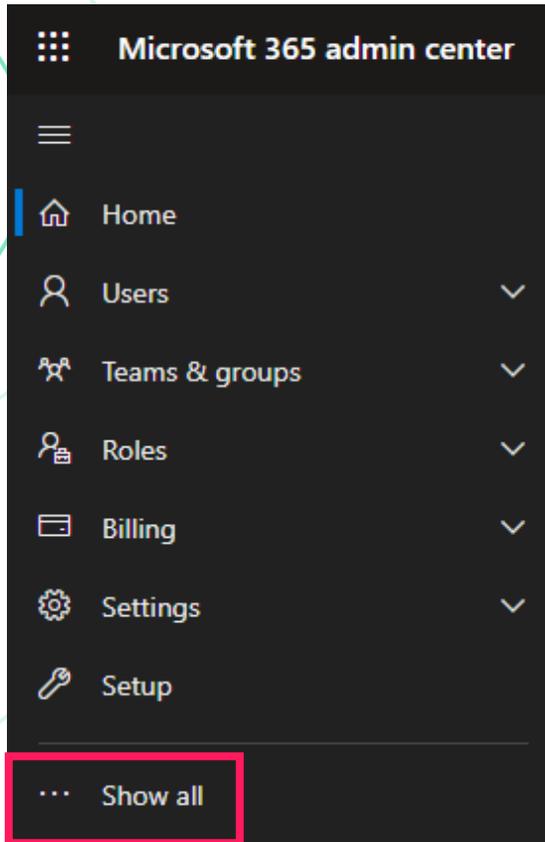
Password

[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 *

IdeaDemoRoom

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

Email *

IdeaDemoRoom

@

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.

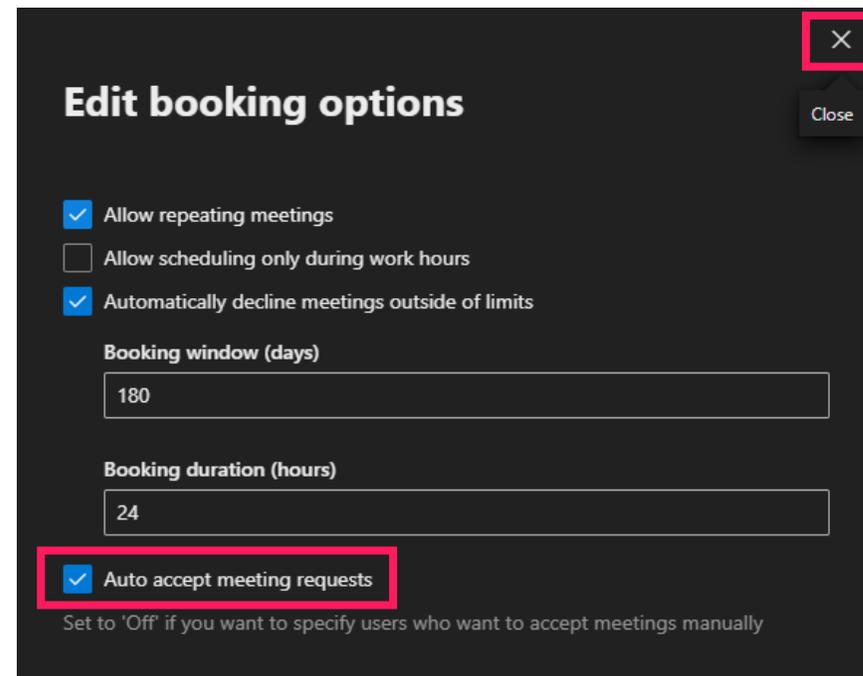
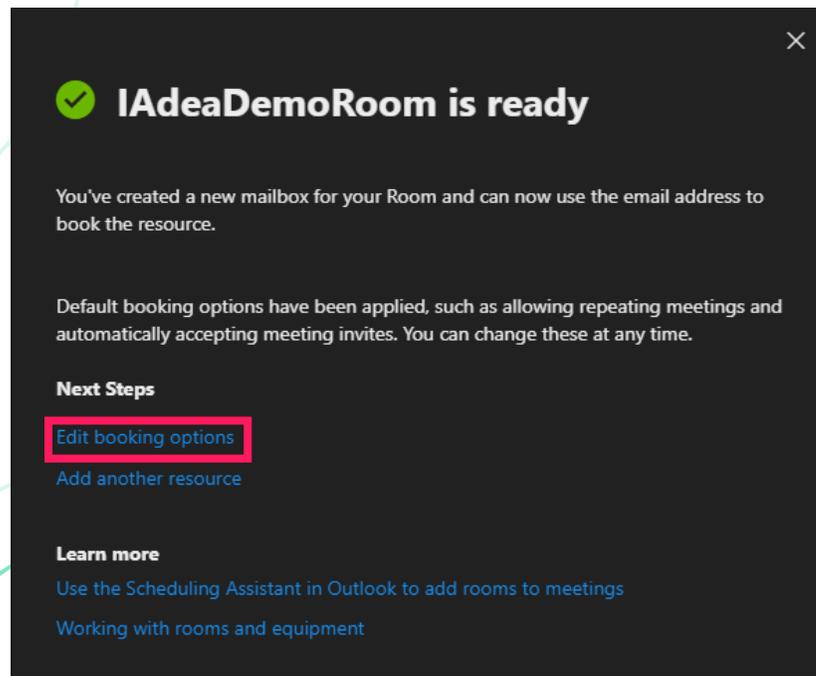
Location

Phone number

Save

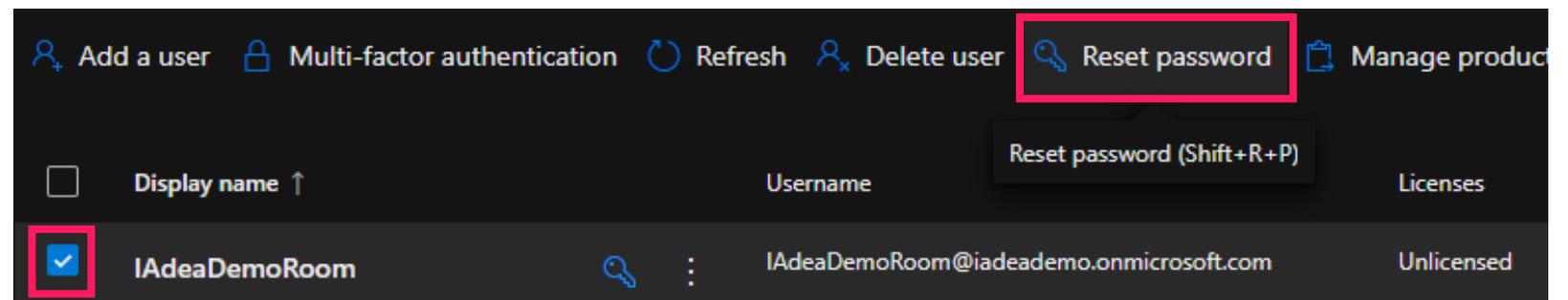
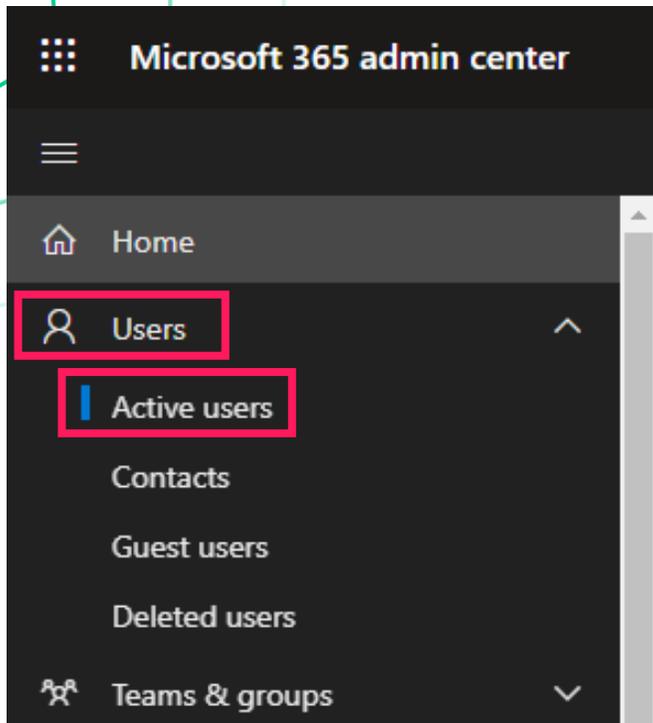
4. Adjusting Booking Preferences

- 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

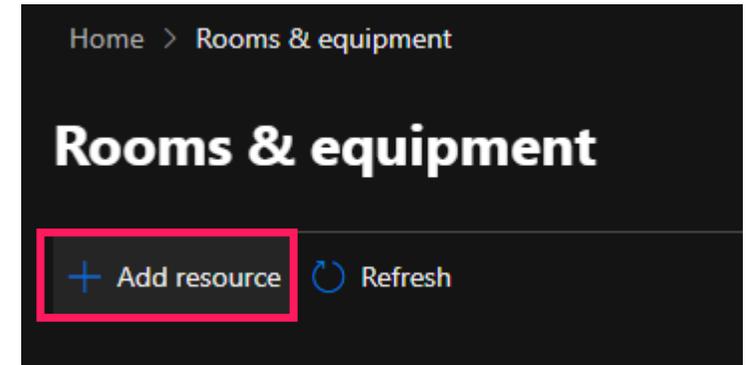
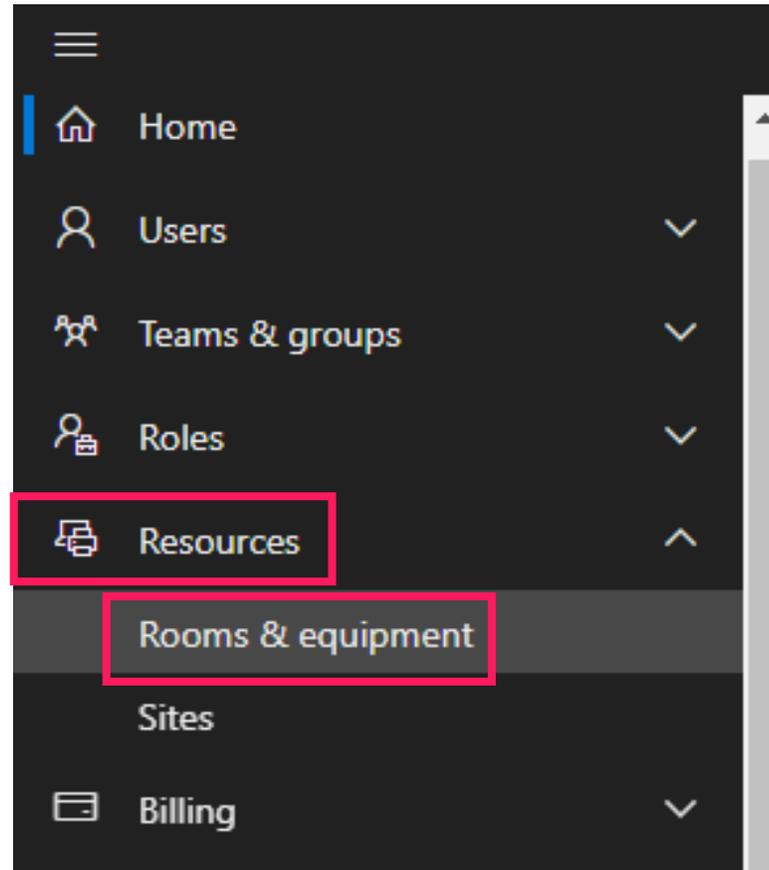
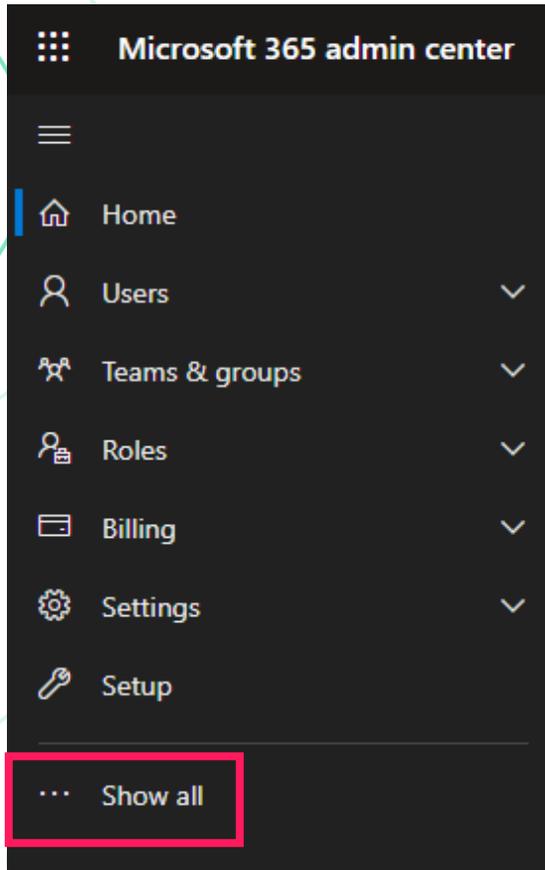
Your email *

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.

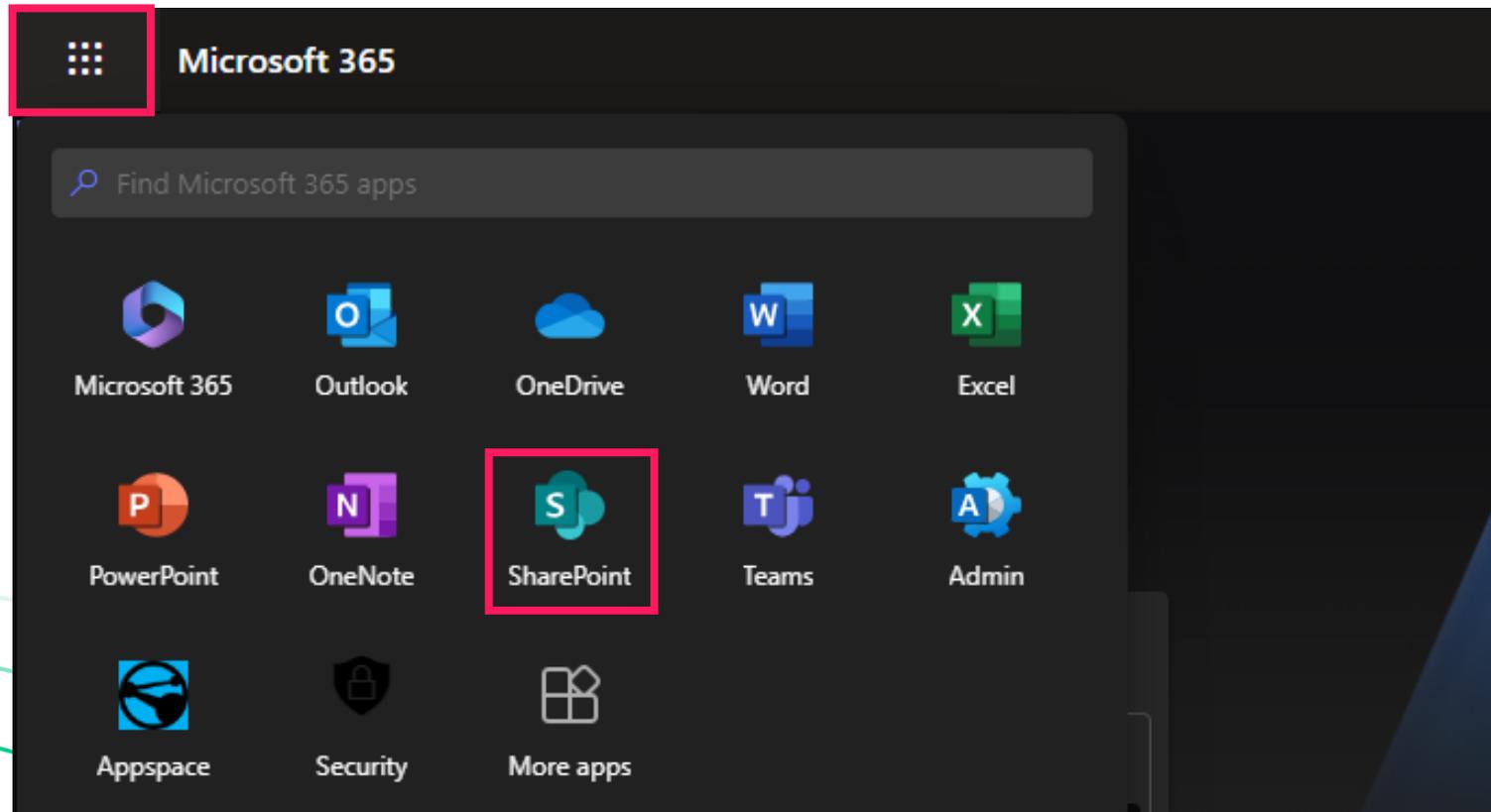


Step 2. Identifying the SharePoint Root Site

- Access SharePoint through Office365
 - Identify the Root Site

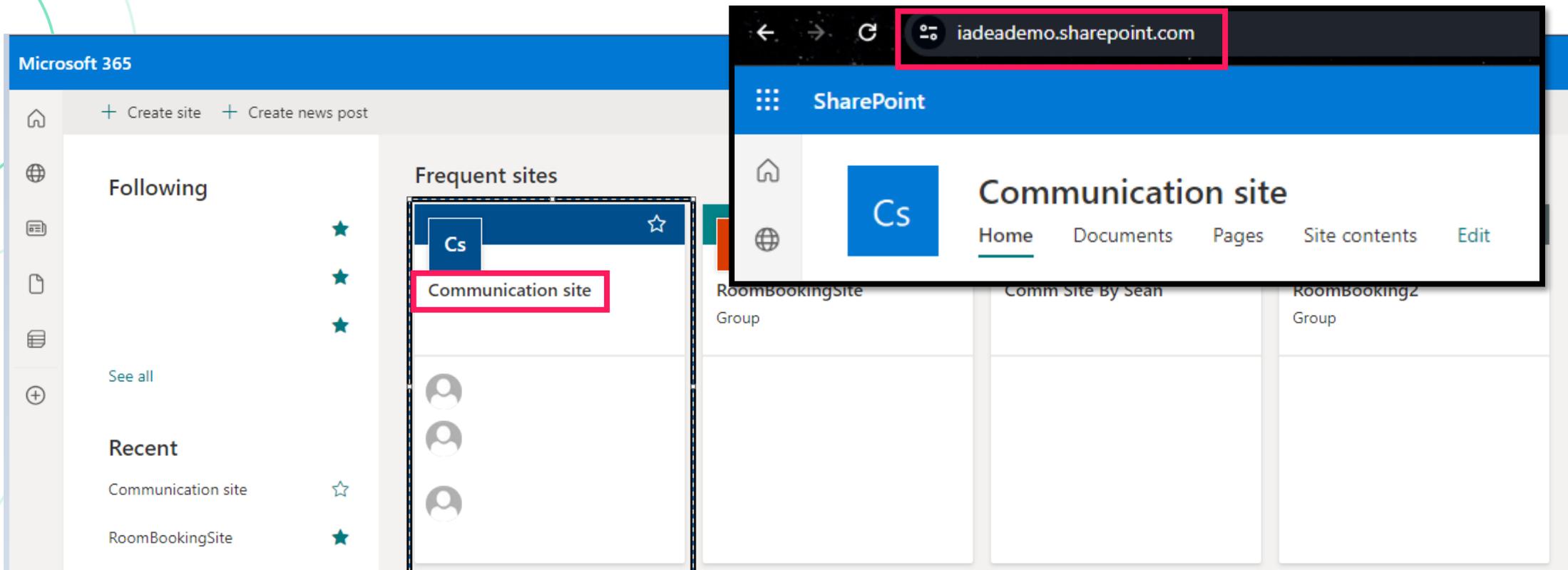
1. Accessing Office365 and Launching SharePoint

- 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'.

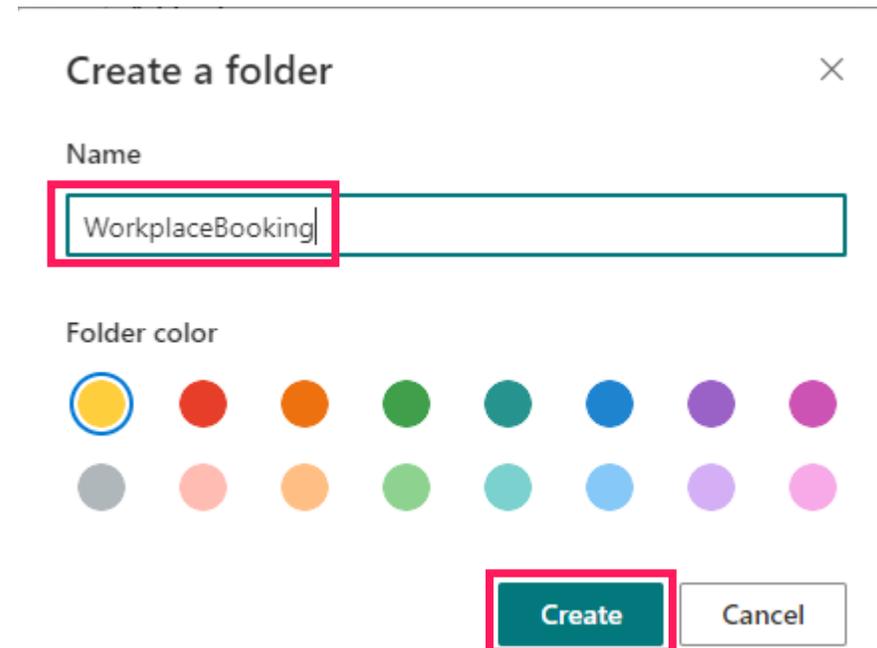
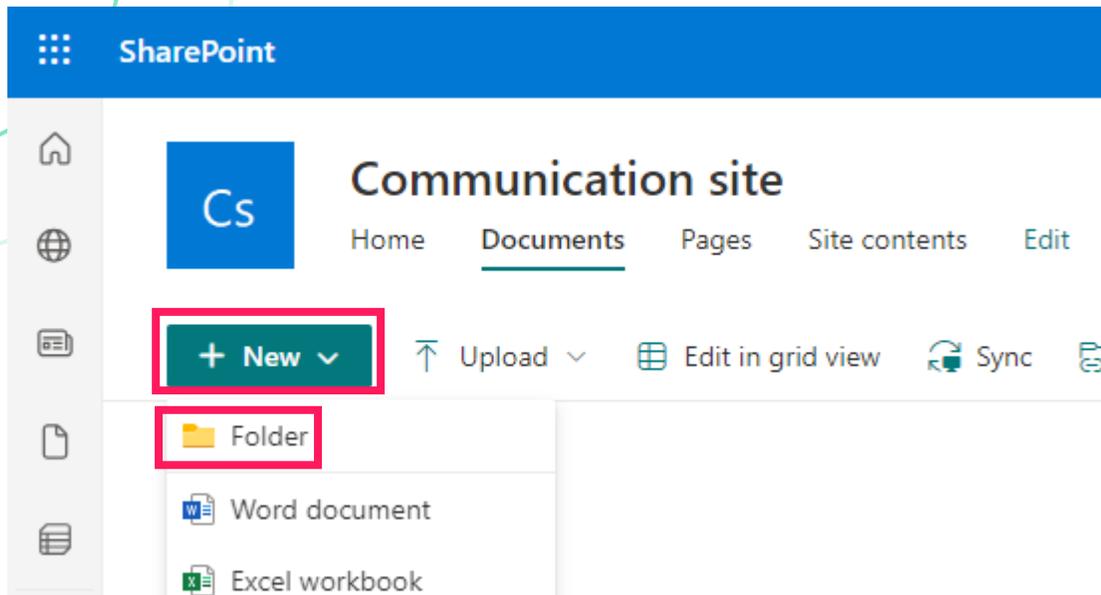


Step 3. Configuring Files on SharePoint

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

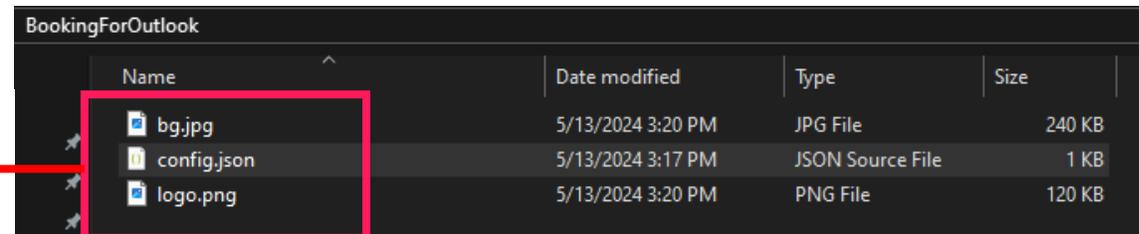
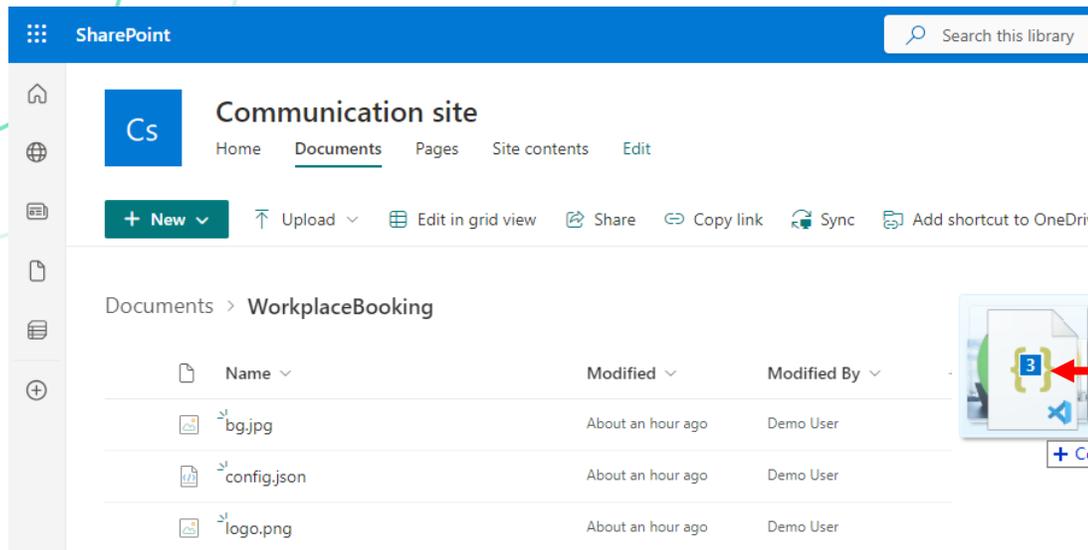
1. Creating a New Folder Named WorkplaceBooking

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



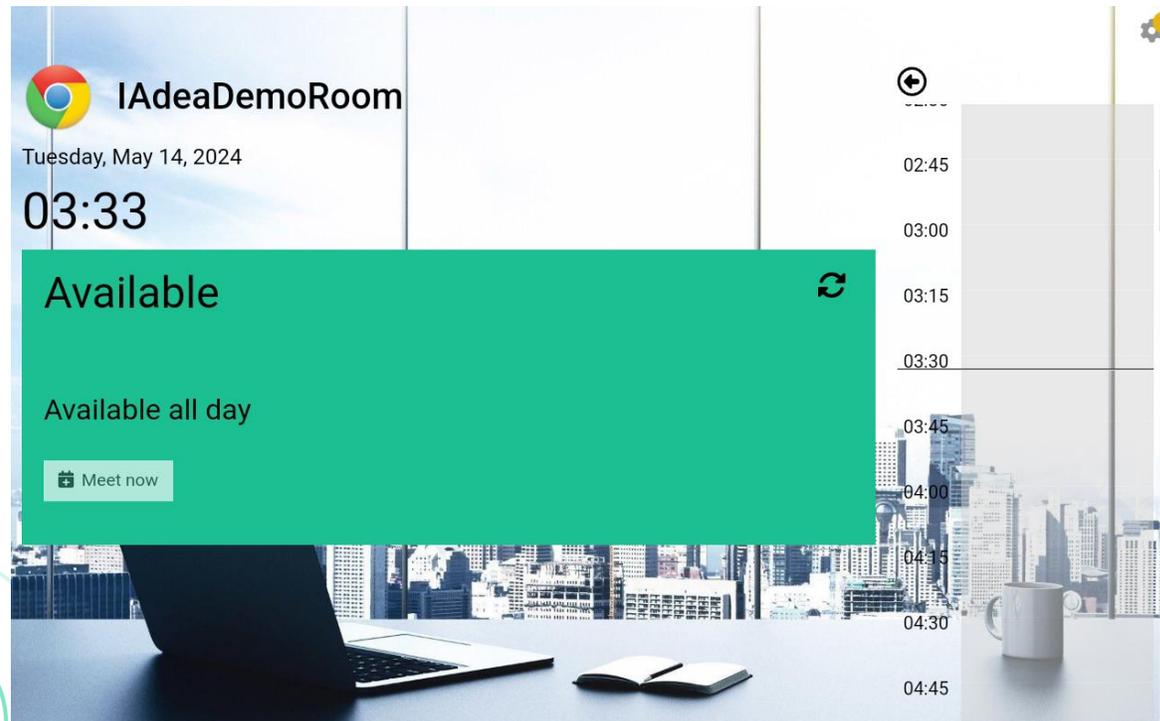
2. Pasting Config and Image Files

- 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.



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>

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

Enterprise Application

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. 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]

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation options like 'Diagnose & solve problems', 'Identity', 'Users', 'Groups', etc. The main content area is titled 'IAdea Booking (for Outlook) | Permissions'. A red box labeled '3' highlights the 'Grant admin consent for IAdea America Corp.' button. Below this, a table lists permissions for Microsoft Graph. A red box labeled '2' highlights the 'User.Read' permission. At the bottom right, a consent dialog is shown with a red box labeled '4' highlighting the 'Accept' button.

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			

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.

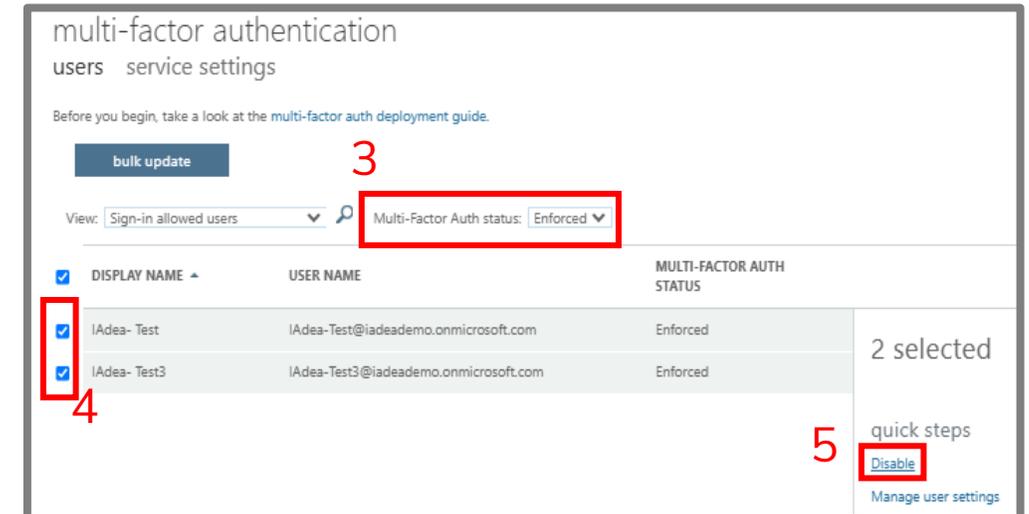
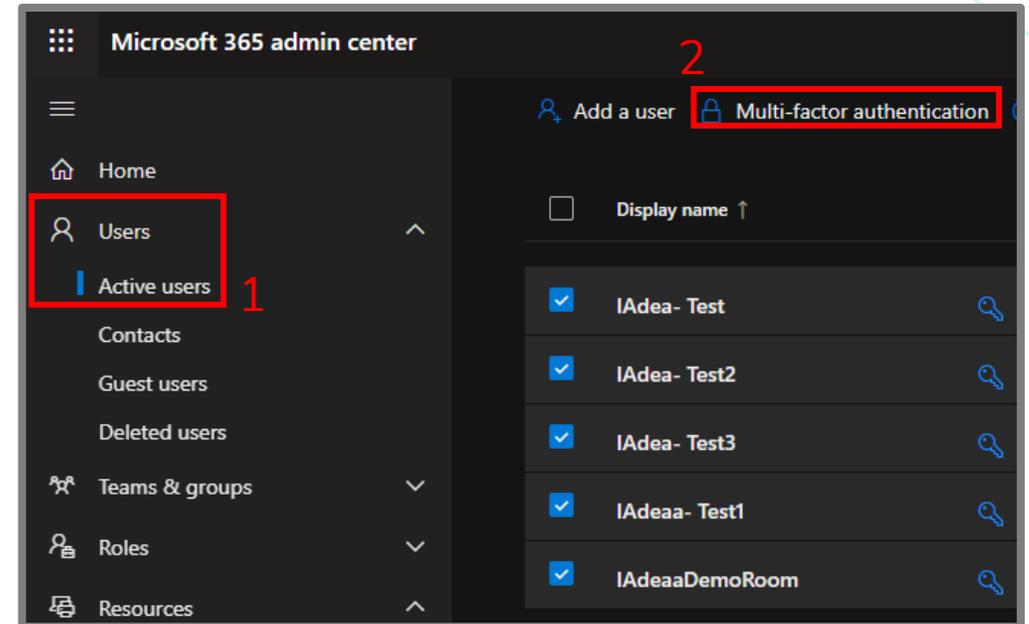
2a. Disable Per-User MFA in MS365 Admin Center

- **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

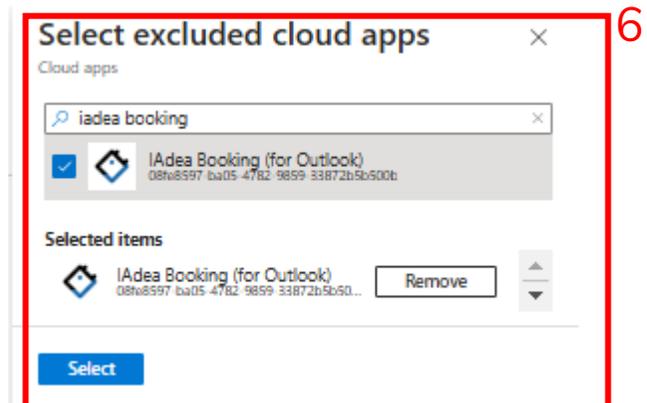
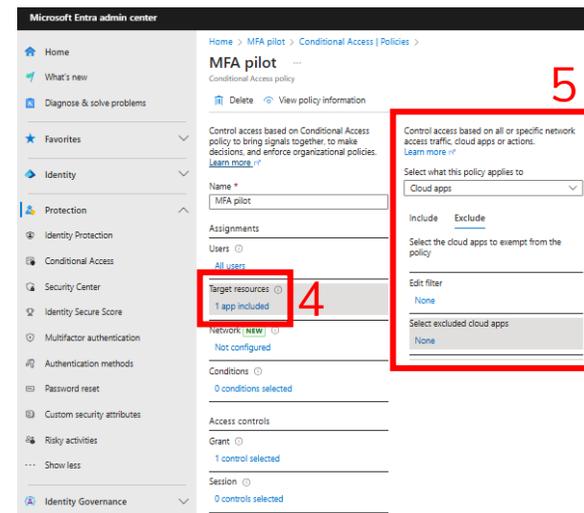
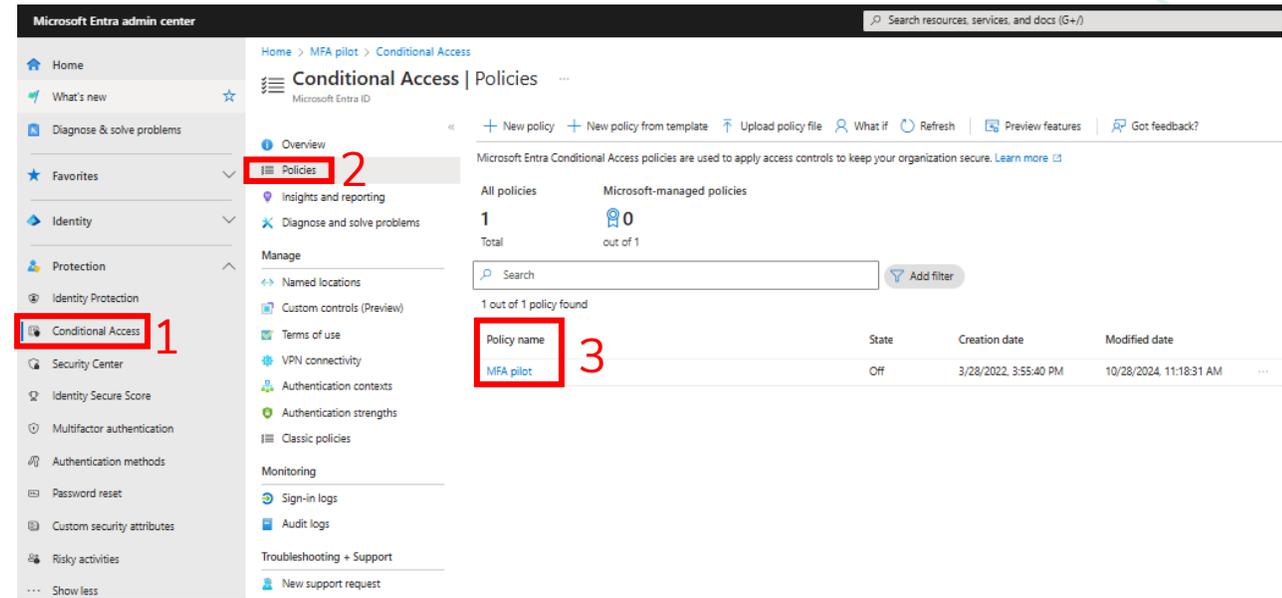
If you've previously turned on per-user MFA, you must turn it off before enabling Security defaults. You should also turn off per-user MFA after you've configure your policies and settings in Conditional Access.

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](#)

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
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
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)

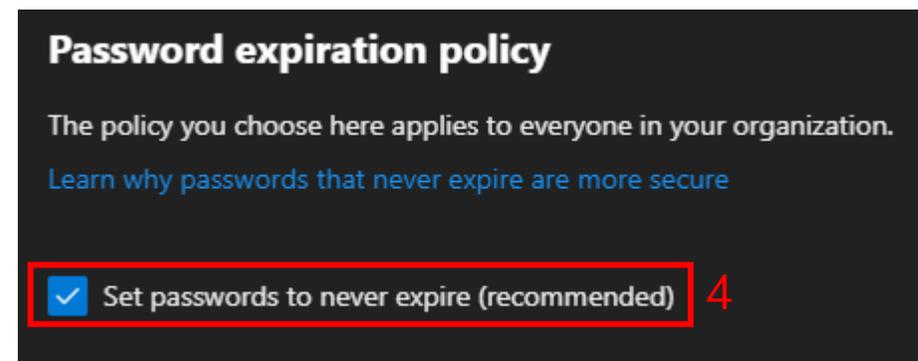
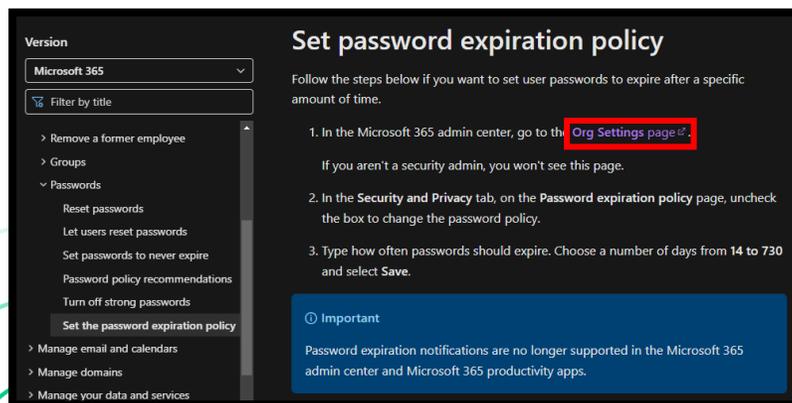
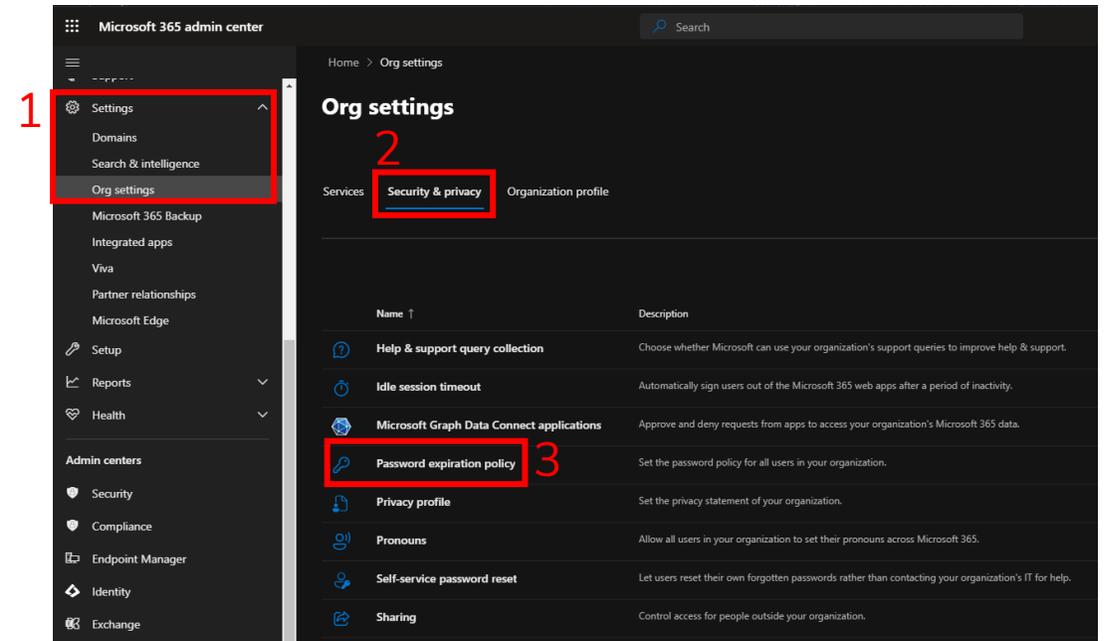
1. Connect to Active Directory PowerShell:

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

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-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>
 - Step 1: Download [ip-ranges.json](#) file on the website
 - Step 2: Find ["service": "CLOUDFRONT"] and it will display several IP ranges
 - 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](#)

The image shows two screenshots. The top screenshot is from the AWS documentation page for Amazon Virtual Private Cloud (VPC) User Guide. It features a search bar at the top and a navigation breadcrumb: AWS > Documentation > Amazon VPC > User Guide. A sidebar on the left contains a search box and a list of recently added items, including 'Delete a security group' and 'Configure security group rules'. The main content area is titled 'Download' and contains instructions on how to download the 'ip-ranges.json' file. A red box labeled 'a)' highlights the 'ip-ranges.json' link. The bottom screenshot shows a 'Pretty-print' JSON viewer. The JSON content is displayed with syntax highlighting. A red box labeled 'b)' highlights the '"service": "CLOUDFRONT"' entry in the JSON, which is also highlighted in yellow in the original image.

```
aws
Search in this guide
Contact

AWS > Documentation > Amazon VPC > User Guide

Amazon Virtual Private Cloud
User Guide

Recently added to this guide
Preview
Delete a security group
July 27, 2024
Configure security group rules
July 27, 2024

Download

To view the current address ranges, download ip-ranges.json. To maintain history, save successive versions of the JSON file on your own computer. To determine whether there have been changes since the last time that you saved the file, check the publication time in the current file and compare it to the publication time in the last file that you saved.

The following is an example curl command that saves the JSON file to the current directory.

Pretty-print
"service": "ROUTE53",
"network_border_group": "GLOBAL"
},
{
  "ip_prefix": "120.52.22.96/27",
  "region": "GLOBAL",
  "service": "CLOUDFRONT",
  "network_border_group": "GLOBAL"
},
{
  "ip_prefix": "205.251.249.0/24",
  "region": "GLOBAL",
  "service": "CLOUDFRONT",
  "network_border_group": "GLOBAL"
},
}
```



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