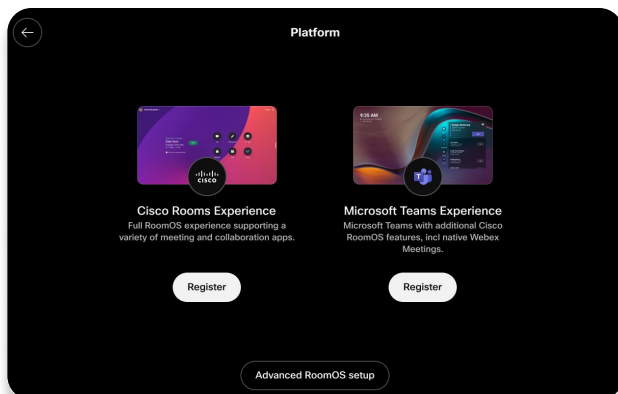


Troubleshooting common issues and challenges

As you deploy your Cisco Devices for Microsoft Teams Rooms, you may experience a few bumps along the way. This guide is here to help you quickly identify and overcome these common issues, ensuring a smooth and successful setup.

Registering your devices

If Microsoft Teams Rooms option isn't available to register, see [Software upgrades from Control Hub for previously registered devices](#).



Pair the Navigator to a Codec

If you're unable to pair the Navigator to a Codec, follow these steps:

1. Sign in to both the Codec and the Navigator with your Microsoft Teams Rooms account.
2. Register the Codec via <https://microsoft.com/devicelogin>, using the code shown on the screen and your account credentials.
3. Repeat this for the Navigator.
4. After signing in, pair the Navigator with the Codec by entering the pairing code displayed on the Codec's screen into the Navigator.

Create or use the correct account

It's important that you don't use a user account for Microsoft Teams Rooms. Instead, create a Microsoft 365 resource account and run the proper PowerShell commands.

Follow these steps to [create and configure resource accounts for shared spaces and devices](#). Microsoft 365 resource accounts are mailbox and Teams accounts that are dedicated to specific resources, such as a room or device. These accounts can automatically respond to meeting invites based on predefined rules. For instance, a conference room resource account can accept or decline meeting invites depending on its availability.



Tip: There's often confusion around where to assign a license or reset a password; this is done via PowerShell or in the Users section in O365 Admin.

Easily join third-party meetings

Are your Webex Meetings missing a displayed name on the screen? Is the join button missing? If so, make sure you [configure your Microsoft Teams Rooms device to join third-party meetings](#).



Configure Intune or conditional access

You may receive vague errors when signing in to a Microsoft Teams Rooms device. This is often due to issues with conditional access rules or Intune compliance policies not being correctly configured.

Common symptoms:

- You can't sign in to Teams on your device, or you get stuck in sign-in loops.
- You're randomly signed out of Teams on your device.
- Microsoft Teams freezes or crashes on your device.

Things to check:



Device enrollment - Intune isn't always properly configured to manage Android-based Microsoft Teams Rooms devices. Make sure the Android device administrator is enabled for device policy management.



Conditional access policies - Conditional access policies ensure that specific conditions must be met before a device can sign in. If a device fails to sign in due to a conditional access policy, troubleshoot by examining the device account sign-in logs.

1. Go to the Azure sign-in portal and find the **User sign-in** tab.
2. Search for the user account or filter by **Teams application** and **Status: Failure**.
3. Select the login failure and view the details of the failure.
4. You can see the **Failure Reason** on the **Basic info** tab.
5. From there you can see under the **Conditional Access** tab the policy list and which policy or policies are failing.
6. Select the **Failure(s)** and review the policy to see why the failure is happening.

Note: This can be tricky for users, especially in Beta, because not all devices may meet the required conditions set by the company.



Compliance policies - Compliance policies are slightly different from conditional access policies; they are more directly related to the device itself. Common issues seen here, especially related to Beta are:

Issue: Encryption - Some devices in Beta are currently not reporting as being encrypted.

Solution: Create a separate Intune Device Compliance policy to filter for those devices and remove encryption check.

Issue: Jailbroken - Some devices in Beta are reporting as Jailbroken/Rooted.

Solution: Create a separate Intune Device Compliance policy to filter for those devices and remove the root check.

Issue: Unsupported policy - Android policies can be created that have requirements that are not supported by Microsoft Teams Rooms.

Solution: Remove the unsupported policy or create a separate policy without those restrictions.