Teams Rooms Pro Management Remote Access

Microsoft Teams Rooms Pro management securely enables Teams Rooms Pro managers with the ability to connect to a Teams Rooms device within the Teams Room Pro Management portal to troubleshoot hardware and software configuration problems on Teams Rooms device unattended. Teams Rooms Pro Management remote access supports all certified Windows-based Teams Rooms that run Windows 11 operating system.

With role-based access controls, your Teams Rooms Pro Management support staff can remotely connect to the Teams Rooms device while unattended when the device is not in a call.

Teams Rooms Pro Management Remote Access capabilities and requirements

Teams Rooms Pro Management has its own role-based access control which helps you manage user access to room resource data in your organization. By assigning roles to your portal users, you can limit what they can see and change. Each role has a set of permissions that determines what users with that role can access and change within your organization.

See Role Base access control in Teams Rooms Pro management portal

- **Requires tenant level opt-in to enable the feature:** By default, remote access is not enabled for your tenant. It must be enabled to assign role-based permissions. You will also need to provide acknowledgement that you are providing permission to enable this feature which will create an audit log record. Microsoft Teams Rooms Pro Management Remote access follows Microsoft privacy policies.

  ATTENTION: Before you enable and configure remote access, consider your privacy and compliance requirements.

- **Requires Teams Rooms Pro management custom role permissions :** By default, Teams Pro management roles **are not** enabled for remote access. If you choose to turn on remote access, you will need to apply the remote access permission to a custom role and assign users and rooms to have access to the feature.

  To create, edit, or assign custom roles, your account must have one of the following permissions:

  - Global Administrator through Azure Active Directory (Azure AD)

    - Teams Rooms Pro Manager through the Microsoft Teams Rooms Pro Management portal

- **Role-based access control (RBAC)**: Admins can set RBAC rules that determine the scope of a Teams Rooms Pro management users' remote access, such as:
    - **VIEW**: The users who can remotely access the device but is limited to only viewing the device console and displays.
    - **MODIFY**: The users will have full range of actions they can do while accessing Teams rooms devices. For example, who can interact with remote keyboard control.

- **Requires Teams Rooms Pro management portal login:** To use remote access, the Teams Room Pro management custom role user must sign into the Teams Rooms Pro management portal from your organization. You can't use remote access to access Teams Rooms devices outside of the Teams Rooms Pro management portal.

- **View details about past sessions**: In the Teams Rooms Pro management portal, you can view audit logs that include details about who connected to the room device, on what device, and for how long.

Pre- Requisites for Teams Rooms Remote Access

The following general prerequisites apply to Teams Rooms Pro Management remote access:

- Teams Rooms Pro license for the Teams Rooms device
- Supported Microsoft Teams Rooms on Windows (see Teams Rooms Certified Devices)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) (agent will install if not present or below version 14.20.27305.0 at first remote access session)
- Teams Rooms Pro management remote access uses Azure Communication Services. Learn more on how to Prepare your organization's network for Azure Communication Services - An Azure Communication Services concept document | Microsoft Learn

- Add the following URLs, if they are not already in your network allowlist:
    - https://mmrprod**noam**pubsub.webpubsub.azure.com
    - https://mmrprod**emea**pubsub.webpubsub.azure.com
    - https://mmrprod**apac**pubsub.webpubsub.azure.com

Limitations

Teams Rooms Pro management remote access has the following limitations:

- Not supported in GCC, GCC-High or DoD Tenants
- Not supported in Teams Rooms multi-tenant management portal

- You cannot establish a Teams Rooms Pro management session from one tenant to a different tenant.
- May not be available in all markets or localizations.

Supported platforms, browsers and devices

This feature applies to:

- Windows 11 on Teams Rooms for Windows
- Android on Teams Rooms for Android (coming soon)
- Edge browser

Data and privacy

Microsoft logs a small amount of session data to monitor the health of the remote access sessions. This data includes the following information:

- Start and end time of the session. This information is stored on Microsoft servers for 180 days.
- Who accessed what device. This information is stored on Microsoft servers for 180 days.
- Errors arising from remote access sessions themselves, such as unexpected disconnections. This information is stored on Microsoft servers for 180 days.
- Teams Rooms Pro management remote access logs session details about the user accessing the Teams Rooms device. Microsoft can't access a session or view any actions or keystrokes that occur in the session.
- A Teams Rooms Pro management remote access session cannot be established while the device is in a call.
- When a Teams Rooms Pro management user accesses the device, a red-ring visual cue will be displayed on the device for anyone seeing the device in the room.
- When a Teams Rooms Pro management user remotely accesses the device, audio will not be enabled.

Note: No Windows services are required as an external dependency for remote access.

Configure Remote Access for your Teams Rooms Pro Management tenant

To configure your tenant for remote access, review and complete the following tasks:

Task 1: Enable Remote Access

1. Sign in to Teams Rooms Pro Management portal and go to **Settings** > **Remote Access**.

2. Under the **Remote Access** section:
    a. Set **Enable Remote Access** to **Enabled** to allow the use of remote access in your tenant. By default, this setting is *Disabled*.
    b. Enter **email address** of the Admin user acknowledging enabling this feature.
3. Select **Save**.

Task 2: Configure Permissions for Remote Access

By default, the Teams Rooms Pro Manager role will ***not*** have remote access permissions enabled.

From the Teams Rooms Pro manager portal navigation, under **Settings/Roles:**

1. **Create a Custom role**: You must create a custom role to grant remote access to any Pro Management Admin, Site Lead and Site technicians and to assign the rooms in which they will be allowed to access.

    For more information on using Teams Rooms Pro Management RBAC, see Role-based Access Control.

2. **From the Create Role wizard**: create a name and description for this custom role.
3. **Assign Permissions:** To start a remote access session from Teams Rooms Pro management portal, the role needs the **Remote Access** view or modify permissions on the role assignment.

    There are two new permissions for remote access:

    View – the view permission will allow a remote connection to the device but will not allow for keyboard control. You would only see what is displayed on the Teams Rooms device and displays.

    Modify – the modify permission will allow a remote connection to the device with full control on the device.

NOTE: It is not necessary to apply any additional permissions to this custom role. If a user is already assigned in another role, these new permissions will be added to their existing scope.

4. Create **Assignments:** You can create groups (called assignments) for specific users and for specific devices. **Only users and devices that have been scoped into an assignment will have remote access enabled**.

5. **Finish and Save**

Audit reporting

Teams Rooms Pro managers can run an audit log to identify remote access sessions and users who have remote access permissions. Log history is available under **Settings/General**.

To remotely administer a Teams Rooms device

- In the Teams Rooms Pro management portal, choose **Rooms**.
- Select the room device that you want to remotely administer and then, in the **Rooms** tab, choose **Remote Access** tab.

  Note: if you do not see the Remote Access tab, you do not have permission. Please see your Teams Rooms Pro manager administrator in your organization.

- Select **Start Session** to establish a secure connection to remotely access the device. A pop-out modal window within your current Teams Rooms Pro portal session will be displayed. A session will only be established if:
  - the device is in a monitored state within the Teams Rooms Pro Management portal.
  - the device **is not** in an active call.

  You will have several commands available to control the session:

Command	**Description**
Restart a Device	
Short Cut Commands	(not all known short cut commands are available)
Restart after session	**Enable** (default)- will automatically restart the device at the end of the session **Disable –** will not automatically restart the device at the end of the current session. The next session will reset the value to Enable.
Help	Links to this documentation
Displays	MTR Console Front of Room Display 1 Front of Room Display 2 (if applicable)
Enter full screen	Expand the modal window to enter full screen Press **Esc** to exit full screen mode

End session	Terminates the session

For those who have view only access, you will not have the ability to interact with the Teams Rooms device but can use the commands listed above.

For those who have modify access, you can interact with the device.

Security and privacy for remote access in Teams Rooms Pro Management

This topic contains security and privacy information for remote access in Teams Rooms Pro Management.

Security best practices for remote access

Use the following security best practices when you manage Microsoft Teams Room devices using Teams Rooms Pro Management remote access.

Security best practice	More information
Do not enter passwords for privileged accounts when remotely administering the device.	When accounts and passwords are required, have care who uses them.
If you log off the Skype user during a remote access session and log on as a different user, ensure that you log off before you disconnect the remote access session.	If you do not log off in this scenario, the session remains open and visible in the room.
Limit the Permitted Viewers list.	Local administrator rights are not required for a user to be able to use remote control.

Privacy information for Teams Rooms Pro Management remote access

Microsoft Teams Rooms Pro Management Remote access follows Microsoft privacy policies. Specifically for this feature:

- There is no active listening on the device
- No processing of passwords
- Just in Time (JIT) session enabled

Before you configure remote access, consider your privacy, security and compliance requirements.

Terms of Use

Microsoft reserves the right to update and modify this feature at any time without notice to you. The current licensing model allows unlimited number of sessions, however this could change in the future. See Microsoft Terms of Use here.