**Microsoft Teams Rooms**

These are consolidated instructions from Microsoft. Created this document so it would be readily available instead of having to search for it. To set this up, just follow straight down the document and skip the parts you don’t need.

**Plan Microsoft Teams Rooms**

This article introduces an end-to-end approach to planning, delivering, and operating Microsoft Teams Rooms as part of your overall meeting and conference room strategy.

You’ll find planning information below covering the recommended approach and key decisions that you need to make, with links to supporting technical information. We recommend that you review the Plan, Deploy, and Manage sections even if you’re already fully deployed

Microsoft Teams Rooms provides a complete meeting experience that brings HD video, audio, and content sharing to meetings of all sizes, from small huddle areas to large conference rooms.

[Microsoft Teams Rooms help](https://support.office.com/article/Skype-Room-Systems-version-2-help-e667f40e-5aab-40c1-bd68-611fe0002ba2) is a great resource to find out more about Microsoft Teams Rooms and how it can add value as part of your deployment. In addition, we recommend watching this [overview video](https://youtu.be/tNey5KZVCl0).

**Microsoft Teams Rooms components**

Microsoft Teams Rooms includes the following key components to deliver a great user experience:

* Touchscreen control panel
* Compute
* Microsoft Teams Rooms application
* Dock/extender
* Peripheral devices (camera, microphone, speaker)
* External screens (maximum of two)
* HDMI input

You can procure these components as preinstalled bundles from a number of vendors, or you can purchase the supported components individually by following the [requirements documented in this article](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/requirements).

In addition to the Surface Pro/dock combination, you can also purchase Microsoft Teams Rooms with the touchscreen control panel, compute, dock, and key peripheral devices integrated.

Typically, the bundles and integrated units include preinstalled software, whereas if you buy supported components individually for the Surface Pro systems, you’ll need to install the software. For instructions, see [this article about installing software on devices](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-scale).

You can deploy Microsoft Teams Rooms with Microsoft Teams, Skype for Business Online, or Skype for Business hybrid or on-premises deployments. See [Microsoft Teams Rooms Licensing](https://docs.microsoft.com/en-us/SfbOnline/skype-for-business-and-microsoft-teams-add-on-licensing/license-options-based-on-your-plan/skype-room-systems-v2.md) for information on the needed licenses.

|  |  |
| --- | --- |
|  |  |
| Decision points | * Will you deploy Microsoft Teams Rooms in your organization? * How will you procure your Microsoft Teams Rooms systems—bundled, as separate components, or as an integrated unit? |
| Next steps | * Identify who will undertake the key activities throughout your deployment. * Review the meeting rooms you have (and plan to set up) to understand where you want to deploy Microsoft Teams Rooms and the peripheral devices that would be appropriate for the room size. |

**Identify who will undertake the key activities throughout your deployment**

Use the approach illustrated below to guide you through your deployment, and customize the sample outputs provided throughout these articles as needed for your organization.

Begin with understanding what conference rooms you have and envisioning what would work best for you in the future, then move through selecting and procuring the equipment you need, readying your sites, configuring and deploying your service, managing change and user adoption, and developing operations and maintenance procedures.

You might need to coordinate these activities across several teams. We provide a high-level view of the main activities that you should cover, and also suggestions for the teams who are typically involved in deploying and managing conference room systems, to help you decide who you need to work with.

**Room inventory and capability planning**

The first step is to inventory your organization’s existing meeting and conference rooms to understand their environment, room size, layout, and purpose, and to identify the capabilities you want each room in scope to have in the future such as which richer collaboration capabilities will be enabled in the room.

After you create an inventory of the equipment and capabilities in each existing room, your requirements for that room feed into your device selection planning to create a rich conferencing solution. The modalities (audio, video) needed for each room—in addition to room size and purpose—all play an important role in deciding which solution is most appropriate for each room.

As part of your discovery, it’s key to consider room acoustics and layout. For example, check that the chairs in the room won’t block the camera view. Verify that the room doesn’t have excessive echo or noisy air conditioning, and that it does have sufficient power for the screens and Microsoft Teams Rooms. There are many factors to consider that your audio-visual (AV) team or partner will be able to advise on.

Decision points

* Which rooms are in scope for this deployment?
* Which sites are in scope for your deployment?
* Who will undertake the meeting rooms inventory?

Next steps

* Review the rooms in scope, and define Microsoft Teams Rooms configurations for them

**Pro Tip** – If you have many sites to inventory, you might want to download and use the [Site Rollout and Migration Planning - Site Questionnaire](https://myadvisor.fasttrack.microsoft.com/CloudVoice/Downloads?SelectedIDs=5_1_0_15).

**Device selection**

Evaluate which Microsoft Teams Rooms solution is the most suitable for each room based on the future capabilities you want for the room. Decide which AV peripheral devices are the best fit, depending on room size and layout.

For guidance for the type of system and peripheral devices by room type and size, see the [Microsoft Teams Rooms requirements](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/requirements) article.

Based on the vendor you prefer, use the information provided in the requirements article to define your Microsoft Teams Rooms and supported peripheral device configuration per room type, and use this as a template for your deployment.

**Pro Tip** – Some room types might not be applicable for your deployment.

Decision points

* From your inventory, which types of rooms are in scope for your deployment?
* From your inventory, which types of rooms are in scope for your deployment?

Next steps

• Start to gather key operational material for your chosen systems, and engage your procurement team.--

**Pro Tip –** Now is a great time to start gathering information about the Microsoft Teams Rooms solution you’ve chosen. We recommend that you work with your vendor to discuss completing the design template to capture information that will be relevant to your deployment; you can [download this handy template](https://myadvisor.fasttrack.microsoft.com/CloudVoice/Downloads?SelectedIDs=4_4_0_11) from MyAdvisor.

**Procurement**

You can procure your chosen system as a bundle or an integrated solution via device partners. You can also acquire a partner device dock and prepare your own Microsoft Teams Rooms solution by using a Surface Pro device and existing, *supported* AV peripheral devices.

You can acquire Microsoft Teams Rooms from a number of partners who are listed in the [requirements article](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/requirements). Please visit the partners’ websites to learn more about these solutions and procurement options.

Depending on your deployment scale and approach, you might decide to have the Microsoft Teams Rooms and supported peripheral devices shipped to a central location for initial configuration and assignment. This might be a good approach for a staged rollout across many sites. Or, you might choose to ship the bundles directly to your sites.

Decision points

* Will you ship the components directly to a site or to a staging facility?
* Who will manage the staging facility (if you decide to use one)?

Next steps

* Plan for operations.
* Plan for adoption and change management.

**Plan for operations**

Your organization must execute monitoring, administration, and management tasks on an ongoing basis, and it’s key to agree who will undertake these tasks early in your deployment.

Many organizations have an AV team or partner who manages their conference rooms and devices. This team should be involved in agreeing who will manage the Microsoft Teams Rooms devices going forward to monitor performance, and deploy software updates and hotfixes.

Consider which helpdesk queue you’ll route Microsoft Teams Rooms֪–related calls to, and provide an FAQ to the helpdesk team so they can better understand how to use Microsoft Teams Rooms and the key troubleshooting steps they can take. A good starting point for this FAQ is the [user help](https://support.office.com/article/Skype-Room-Systems-version-2-help-e667f40e-5aab-40c1-bd68-611fe0002ba2) and the [known issues list](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/known-issues).

Decision points

* Decide who will manage Microsoft Teams Rooms.
* Decide which helpdesk queue to route Microsoft Teams Rooms–related calls to.

Next steps

* Prepare to host accounts.

**Plan for adoption and change management**

Microsoft Teams Rooms systems introduce new capabilities to your users. It’s important that you recognize that this will be a change for your users, and you should ensure your campaign identifies the benefits the new system will have for your users and the key talking points leads can use to discuss with their teams.

Consider scheduling show-and-tell events and poster drops at each site to inform your users of the new capabilities. You might also create in-room “quick start guides.” Consider finding a meetings champion on each site who can help others get up to speed and start using the devices.

**Microsoft Teams Room app version support**

Microsoft plans to release updates for Microsoft Teams Rooms a few times per year with each update supported for twelve (12) months from its general availability (GA) release date. Technical support will be provided for the entire twelve (12) months. However, our support structure is now dynamic, evolving into two distinct servicing phases that depend on the availability of the latest version.

**Servicing and Critical Updates servicing phase** - When running the latest version of Microsoft Teams Rooms, you will receive regular updates, that contain Security and Servicing updates.

**Security Updates (Only) servicing phase** - After a new version is released, support for older branches will reduce to Security updates only for the remainder of the twelve (12) month Servicing Updates support lifecycle.

**Note**

The latest version is always in the Servicing and Critical Updates servicing phase. This means that in the event that you encounter a code defect that warrants a critical update, you must have the latest version installed in order to receive a fix. All other supported versions will only be eligible to receive security updates.

All support ends after the twelve (12) month lifecycle for a version has expired or if more than two updates have been released since then. At that time, customers must update to a supported version.

All releases are listed in the [Microsoft Teams Rooms release notes](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/srs2-release-note).

**OS Version support**

Windows 10 feature updates for devices running Microsoft Teams Rooms are not offered for 6 months from the time when Windows makes a release update. This is accomplished by putting a special block for Microsoft Teams Rooms devices on Windows Update for Business channel (i.e. Semi-Annual Channel) and through the app settings. During this blocked period Microsoft performs various tests both in house and through our device OEM partners to make sure that new Windows 10 feature release is working in harmony with the Microsoft Teams Rooms app and peripherals connected to it. This is important to both ensure device security, consistent user experience and to make sure quality of experiences offered through Microsoft Teams Rooms app.

From the time block is lifted (i.e. Window 10 feature update is offered to download on these devices), Microsoft Teams Rooms supports the specific Windows 10 feature release for 12-month period in line with App support policy. Since Windows 10 feature updates are offered about every 6 months, this also means that Microsoft Teams will have two additional releases to test by the time support for current version is ended. This also means that a Windows 10 version will be unblocked every 6 months to all Microsoft Teams Rooms customers. As we are continuously making app changes and are developing against last unblocked Windows release, in some cases need to take dependency on Windows features available in newer versions of Windows and the fact that it makes it harder for Microsoft to make changes to the version that is 12-18 months old. To ensure you get the app fix for an issue your encounter on your Microsoft Teams Rooms device, we urge all customers to upgrade these devices to latest Windows 10 feature update offered to stay within supported windows version guidance.

As such, Microsoft Teams Rooms devices require Windows 10 version 1709 as the minimum supported version starting May 2019. No new app releases will be offered to systems on Windows 10 Versions 1703 or below.

**Note**

When a Microsoft Teams Rooms device is compatible with the next version of Windows 10 OS, the device automatically updates to the next version through Windows Update. Microsoft Teams Rooms devices should not be upgraded to the next release of Windows 10 manually or via enabling Windows Update for Business (WUFB) group policies using the “Select the Windows readiness level for the updates you want to receive” and "Select when Preview Builds and Feature Updates are received" options through a GPO. Enabling these group policies is known to lead to issues between Windows 10 OS update and the Microsoft Teams Rooms app.

**Prepare your environment**

This section contains an overview of the steps required to prepare your environment so that you can use all of the features of Microsoft Teams Rooms.

1. Prepare a device account for each Microsoft Teams Rooms console. See [Deploy Microsoft Teams Rooms](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2) for details.
2. Ensure that there is a working network/Internet connection for the device to use.
   * It must be able to receive an IP address using DHCP. (Microsoft Teams Rooms cannot be configured with a static IP address at the first unit startup, but afterwards static IP for the device could be configured on the device or on the upstream switch or router.)
   * It must have these ports open (in addition to opening the normal ports for media):
   * HTTPS: 443
   * HTTP: 80
   * If your network runs through a proxy, you'll need the proxy address or script information as well.  
       **Note** Microsoft Teams Rooms does not support HDCP input, which has been observed to cause issues with HDMI ingest functionality (video, audio). Take care to ensure that switches connected to Microsoft Teams Rooms have HDCP options turned off.
3. In order to improve your experience, Microsoft collects data. To collect data, we need these sites whitelisted:
   * Telemetry client endpoint: <https://vortex.data.microsoft.com/>
   * Telemetry settings endpoint: <https://settings.data.microsoft.com/>

**Create and test a device account**

A *device account* is an account that the Microsoft Teams Rooms client uses to access features from Exchange, like calendar, and to enable Skype for Business. See [Deploy Microsoft Teams Rooms](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2) for details.

**Check network availability**

In order to function properly, the Microsoft Teams Rooms device must have access to a wired network that meets these requirements:

* Access to your Active Directory or Azure Active Directory (Azure AD) instance, as well as your Microsoft Exchange and Skype for Business servers.
* Access to a server that can provide an IP address using DHCP. Microsoft Teams Rooms cannot be configured with a static IP address.
* Access to HTTP ports 80 and 443.
* TCP and UDP ports configured as described in [Port and protocol requirements for servers](https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/ports-and-protocols) for on-premise Skype for Business Server implementations, or [Office 365 URLs and IP address ranges](https://support.office.com/en-us/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2?ui=en-US&rs=en-US&ad=US) for Microsoft Teams or Skype for Business online implementations.

**Important**

Be sure to use a wired 1 Gbps network connection to assure you will have the needed bandwidth.

**Certificates**

Your Microsoft Teams Rooms device uses certificates for Exchange Web Services, Microsoft Teams or Skype for Business, network usage, and authentication. If the related servers use public certificates, which is the case for Online and some On-Premises deployments, there should be no further action required on the part of the admin to install certificates. If, on the other hand, the certificate authority is a private CA (typical for On-Premises deployments) then the device needs to trust that CA which means having the CA + CA chain certificates installed on the device. Adding the device to the domain may perform this task automatically.

You will install certificates the same way you would for any other Windows client.

**Note**

Certificates may be required in order to have Microsoft Teams Rooms use Skype for Business Server.

**Proxy**

Microsoft Teams Rooms is designed to inherit Proxy settings from the Windows OS. Access the Windows OS in the following manner:

1. In the Microsoft Teams Rooms UI, click on the Settings gear icon where you'll be prompted for the local Administrator password on the device (the default password is **sfb**).
2. Tap on **Settings** followed by tapping on the **Go to Windows** button and then tapping on the **go to Admin Sign In** button and then clicking the **Administrator** button (if the computer is domain joined choose **Other User,** then use .\admin as the user name).
3. In the **Search Windows** box bottom left type in regedit (either long press the screen or right click and choose **Run as administrator**).
4. Click on the HKEY\_USERS folder (you'll see a list of machine user SIDs) ensure the root folder HKEY\_USERS is selected.
5. Click on File and then choose **Load Hive.**
6. Browse the to the **C:\Users\Skype** folder and type in the File name box NTUSER.dat and press the open button
7. You'll be prompted for a Key Name for your newly loaded Hive; type in Skype (you should now see the registry settings for the Skype User).
8. Open the Skype key and browse to HKEY\_USERS\Skype\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings then ensure these settings are entered:  
    [HKEY\_USERS\Skype\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings]  
    "MigrateProxy"=dword:00000001  
    "ProxyEnable"=dword:00000001  
    "ProxyServer"="xx.xx.xx.xx:8080"  
    If ProxyServer doesn't exist you may have to add this key as a string, change the xx.xx.xx.xx:8080 to the ip/host and port of your Proxy server.
9. Once you are finished making your changes highlight the Skype User key (root folder for Skype) and choose unload Hive from the Registry file menu (you'll be prompted for confirmation - select **Yes** ).
10. You can now close the registry editor and type logoff into the Windows search box.
11. Back at the sign-in screen, choose the **Skype** user. If all the previous steps were successful, the Microsoft Teams Rooms device will sign-in successfully.

To use this application, you must be able to connect to the endpoints described below. To see the IP addresses, expand the IP address section below the table describing the traffic flow.

**Note**

The wildcard for contoso.com and broadcast.skype.com represents a long list of nodes that are exclusively used for Office 365.

**Create provisioning packages**

You will use provisioning packages to authenticate to Exchange Server or Office 365.

**Admin group management**

After domain joining, you can use Group Policy or the Local Computer Management to set a Security Group as local administrator just like you would for a Windows PC in your domain. Anyone who is a member of that security group can enter their credentials and unlock Settings.

**Note**

If your Microsoft Teams Rooms device loses trust with the domain (for example, if you remove the Microsoft Teams Rooms from the domain after it is domain joined), you won't be able to authenticate into the device and open up Settings. The workaround is to log in with the local Admin account.

**Local accounts**

**Microsoft Teams Rooms Local User Account**

The Device Account does not typically use a password. It is possible to give it a password, but there are consequences, including a possibility that users might get locked out of the console application when that password expires. Consequently, the administrator should take are to ensure that the password is not allowed to expire.

**"Admin" - Local Administrator Account**

Microsoft Teams Rooms default password is set to "sfb". The Password can be changed locally by going to Windows Settings > Go to Windows or in the AutoUnattend.xml file (use the Windows System Image manager from ADK to make the change to the xml file).

**Caution**

Be sure to change the Microsoft Teams Rooms password as soon as possible.

You can also manage the Local Administrator password by setting up a group policy where domain admins are made local admins.

The Local admin password is not included as a choice during Setup.

**Machine Account**

Much like any Windows device, the Machine Name can be renamed by right clicking in Settings > About > Rename PC.

If you would like to rename the computer after joining it to a domain, use the Rename-Computer PowerShell command followed by the computer's new name.

**Microsoft Teams Rooms requirements**

This article summarizes the requirements for supporting Microsoft Teams Rooms.

Your deployment will involve account creation as described in [Deploy Microsoft Teams Rooms](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2)and setting up a meeting console as described in [Configure a Microsoft Teams Rooms console](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console).

* [Skype for Business add-on licensing](https://docs.microsoft.com/en-us/SkypeForBusiness/skype-for-business-and-microsoft-teams-add-on-licensing/skype-for-business-and-microsoft-teams-add-on-licensing)
* [License options based on your plan: Microsoft Teams Rooms](https://docs.microsoft.com/en-us/SkypeForBusiness/skype-for-business-and-microsoft-teams-add-on-licensing/license-options-based-on-your-plan/skype-room-systems-v2)

**Note**

Microsoft Teams Rooms is intended for use with Microsoft Teams, Skype for Business Server 2019, Skype for Business Server 2015, or Skype for Business Online.

Earlier platforms like Lync Server 2013 aren't expected to work with Microsoft Teams Rooms.

**Note**

If using an on-prem Exchange server, Microsoft Teams Rooms requires the use of Exchange Server 2013 SP1 or later.

**Hardware requirements**

Microsoft Teams Rooms can scale to different room sizes through accessories depending on audio and video peripherals. The hardware listed in this article supports both Skype and Teams meeting modes. Audio and video peripherals connect to Microsoft Teams Rooms via a USB or HDMI connection on the docking device. You will also need:

* A 32GB or larger USB disk you will configure as bootable Windows installation media for Windows 10 Enterprise.
* List of supported hardware
* https://docs.microsoft.com/en-us/MicrosoftTeams/room-system/requirements#hardware-requirement

**Microsoft Teams Rooms licenses\**

* The following table lists the licensing-dependant features that are available in Microsoft Teams Rooms and what licenses you need to buy to get them.
* **Note**
* The room that is being set up needs to be a user object and have these licenses assigned to it. The new Meeting Room license is now available in Office 365.

See list of licenses

<https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/skype-room-systems-v2>

**Plan Microsoft Teams Rooms management with Azure Monitor**

This article discusses planning considerations for using Azure Monitor to administer Microsoft Teams Rooms devices in your Microsoft Teams or Skype for Business implementation.

[Azure Monitor](https://docs.microsoft.com/azure/azure-monitor/overview) is a collection of management services that were designed in the cloud from the start. Rather than deploying and managing on-premise resources, Azure Monitor components are entirely hosted in Azure. Configuration is minimal, and you can be up and running literally in a matter of minutes. With some customization work, it can aid in managing Microsoft Teams Rooms conferencing systems by providing real-time notifications of system health or faults for individual room systems, and it can potentially scale up to managing thousands of Microsoft Teams Rooms conference rooms.

This article provides a discussion of the requirements, design/architecture, and implementation best practices needed to implement Azure Monitor based management of Microsoft Teams Rooms conference devices, and provides links to detailed articles on implementing Azure Monitor for Microsoft Teams Rooms and critical reference information for ongoing monitoring of Microsoft Teams Rooms rooms.

**Functional overview**

The Microsoft Teams Rooms app on the console device writes events to its Windows Event Log. A Microsoft Monitoring agent, once installed, passes the information to Azure Monitor service.

Once properly configured, Log Analytics parses the JSON payload embedded in the event descriptions to describe how each Microsoft Teams Rooms system is functioning and what faults are detected.

An administrator using Azure Monitor can get notifications of Microsoft Teams Rooms systems that are offline or are experiencing app, connectivity, or hardware failures as well as knowing if a system needs to be restarted. Each system status is updated frequently, so these notifications are close to real-time updates.

**Azure Monitor requirements**

You must have a valid Azure subscription for Azure Monitor to use Log Analytics feature. See [Get started with a Log Analytics workspace](https://docs.microsoft.com/azure/azure-monitor/learn/quick-create-workspace) to create a subscription for your organization.

Link:

https://docs.microsoft.com/azure/azure-monitor/learn/quick-create-workspace

You should familiarize yourself as necessary on how to use the Log Analytics View Designer. See [Views in Log Analytics](https://docs.microsoft.com/azure/azure-monitor/platform/view-designer) for those details.

https://docs.microsoft.com/azure/azure-monitor/platform/view-designer

**Related Tasks**

1. Once subscribed to Azure Monitor Log Analytics, create custom fields (as described in [Map custom fields](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#Custom_fields)) needed to parse the information that will be sent from Microsoft Teams Rooms consoles. This includes understanding the JSON schema documented in [Understand the log entries](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-manage#understand-the-log-entries).  
    https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#Custom\_fields
2. <https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-manage#understand-the-log-entries>
3. Develop a Microsoft Teams Rooms management view in Log Analytics. You can either [Create a Microsoft Teams Rooms dashboard by using the import method](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#create-a-microsoft-teams-rooms-dashboard-by-using-the-import-method) or [Create a Microsoft Teams Rooms dashboard manually](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#create-a-microsoft-teams-rooms-dashboard-manually).

**Individual Microsoft Teams Rooms Console requirements**

Each Microsoft Teams Rooms console is an app running on a Surface Pro device in kiosk mode (normally, it's configured to be the only app that can run on the device). As with any Windows app, the Microsoft Teams Rooms app writes events like startup and hardware faults to the Windows Event Log. Adding an Microsoft Monitor agent on your Microsoft Teams Rooms device allows these events to be collected. (See [Connect Windows computers to the Log Analytics service in Azure](https://docs.microsoft.com/azure/azure-monitor/platform/agent-windows) for details.)

https://docs.microsoft.com/azure/azure-monitor/platform/agent-windows

**Ongoing management**

While using Azure Monitor to manage your Microsoft Teams Rooms devices, you'll need to understand the information contained in the event logs used by Azure Monitor. See [Understand the log entries](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-manage#understand-the-log-entries) for details on these health messages.

https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-manage#understand-the-log-entries

**Deployment overview**

Deployment of Microsoft Teams Rooms essentially breaks down into phases:

* Confirming that your deployment locations (rooms) meet the deployment dependencies
* Creating Microsoft Teams or Skype for Business and Exchange accounts and assigning them to the console devices (see [Configure accounts for Microsoft Teams Rooms](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-configure-accounts))
* Reimaging Microsoft Surface tablets to work as Microsoft Teams Rooms consoles (see [Configure a Microsoft Teams Rooms console](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console) or [Deploy Microsoft Teams Rooms mass deployment guide](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-scale))
* (Optional) Setting up Microsoft Operations Management Suite for your systems (see [Deploy Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy)
* Setting up consoles in meeting rooms and connecting the peripheral devices you need (see the OEM documentation for your set of devices)

AV techs can be used for the last task, but your organization's IT department will need to do the other parts of the process.

**Site readiness**

While the ordered devices are being delivered to your organization, work with your networking and facilities and AV teams to make sure that deployment dependencies are met and each site and room is ready in terms of power, networking, and display. In addition, make sure the physical installation requirements are met. For physical installation considerations, please visit the vendor’s site and leverage the experience of your AV team when installing and mounting screens and running cabling.

You can find out more about these dependencies in the planning guidance links below:

* [Check network availability](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/srs-v2-prep#check-network-availability)
* [Certificates](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/srs-v2-prep#certificates)
* [Proxy](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/srs-v2-prep#proxy)

**Pro Tip** - If you intend to use proxy servers to provide access to Microsoft Teams or Skype for Business Online, first [review this article](https://docs.microsoft.com/skypeforbusiness/optimizing-your-network/proxy-servers-for-skype-for-business-online). Note that when it comes to Skype for Business traffic over proxy servers, we recommend bypassing proxy servers altogether. Skype for Business traffic is already encrypted, so proxy servers don’t make it more secure. As part of your wider deployment, we recommend that you follow the guidance in [Evaluate my environment](https://docs.microsoft.com/MicrosoftTeams/3-envision-evaluate-my-environment#network-readiness) for bandwidth planning and assessing your network’s suitability for real-time traffic. For all bandwidth planning, use the [MyAdvisor Network Planner](https://myadvisor.fasttrack.microsoft.com/CloudVoice/NetworkPlanner). (We recommend that you create a Microsoft Teams Rooms persona to reflect the intended Microsoft Teams Rooms usage [video, screen sharing, audio] and assign a number of users that matches the number of Microsoft Teams Rooms units to be deployed to each site.)

|  |  |
| --- | --- |
|  |  |
| Decision points | * Confirm that your sites meet the key requirements for Microsoft Teams Rooms. * Confirm that you've provided sufficient bandwidth for each site. |
| Next steps | * Start to plan your device deployment and configuration. |

**Pro Tip -** From a site-by-site planning perspective, you might find the following assets useful. They cover more than just Microsoft Teams Rooms and can be used in a full rollout of Skype for Business Online:

* [Site Rollout/Migration Planning Delivery Guide](https://myadvisor.fasttrack.microsoft.com/CloudVoice/Downloads?SelectedIDs=5_1_0_24)
* [Site Rollout and Migration Planning - Playbook](https://myadvisor.fasttrack.microsoft.com/CloudVoice/Downloads?SelectedIDs=5_1_0_16)  **Note** In the playbook, complete the tasks in the section “4.3 – > Conference Rooms” under the “4-Endpoints” sheet for each site where you’re planning to deploy Microsoft Teams Rooms devices. This will enable you to use the bulk account provisioning script later in the process.

**Service readiness**

To prepare for your Microsoft Teams Rooms deployment, do the following key, central tasks:

* Define Microsoft Teams Rooms service account features.
* Prepare an organizational unit and Active Directory group to hold your Microsoft Teams Rooms machine and service accounts, and—optionally—prepare Group Policy objects (GPOs) to enable PowerShell remoting.

**Define Microsoft Teams Rooms service account features**

Depending on the collaboration scenarios that you’ve decided to enable with your Microsoft Teams Rooms deployment, you’ll need to determine the features and capabilities that you assign to each Microsoft Teams Rooms service account that you enable.

|  |  |  |
| --- | --- | --- |
| **Scenario** | **Description** | **Microsoft Teams Rooms service account feature** |
| Interactive meetings | Using voice, video, and screen sharing; making the Microsoft Teams Rooms a bookable resource | Enabled for Skype for Business, enabled for Exchange (Resource Mailbox) |
| Dial-in conferencing | Enable meetings started *directly* from the Microsoft Teams Rooms console with dial-in conferencing coordinates | Enabled for Audio Conferencing |
| Outbound/inbound PSTN Calling | Enable the Microsoft Teams Rooms console to make and receive PSTN calls | Enabled for Phone System |

For more information about Microsoft Teams Rooms accounts, see [Configure accounts for Microsoft Teams Rooms](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-configure-accounts).

|  |  |
| --- | --- |
|  |  |
| Decision points | * Decide which scenarios you’ll support, and identify licensing requirements for your Microsoft Teams Rooms service accounts. |
| Next steps | * Prepare to host machine and service accounts. |

*Sample Microsoft Teams Rooms service account planning table*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Site** | **Room name** | **Room type** | **Future room capabilities** | **Microsoft Teams Rooms account features** |
| London HQ | Curie | Medium | 1 screen, audio and video plus presentation  Dial-in conferencing access  PSTN access | Enabled for Skype for Business, enabled for Exchange (Resource Mailbox)  Enabled for Audio Conferencing  Enabled for Phone System |
| Sydney HQ | Hill | Large | 2 Screens, audio and video plus presentation  Dial-in conferencing access  PSTN access | Enabled for Skype for Business, enabled for Exchange (Resource Mailbox)  Enabled for Audio Conferencing  Enabled for Phone System |

**Prepare to host Microsoft Teams Rooms machine and service accounts (optional)**

To enable you to manage and report on your Microsoft Teams Rooms machine and service accounts, prepare your on-premises Active Directory or Azure Active Directory (Azure AD).

Define an on-premises Active Directory or Azure AD group to add all Microsoft Teams Rooms service (user) accounts to, and then create usage reports by using the Get-CSUserSession PowerShell cmdlet across your Microsoft Teams Rooms deployment. For example, create a group named SkypeRoomSystemsv2-Service-Accounts.

Define one organizational unit in your on-premises Active Directory or Azure AD hierarchy to hold all Microsoft Teams Rooms machine accounts (if they’re joined to the domain) and one organizational unit to hold all the Microsoft Teams Rooms user accounts. If you do create an organizational unit for the Microsoft Teams Rooms machine accounts, consider disabling inheritance to ensure that you apply only the policies you intended to apply to the domain-joined Microsoft Teams Rooms.

Create a Group Policy object assigned to the organization unit that contains your Microsoft Teams Rooms computer accounts. Use this to:

* [Set power and local account settings](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-operations#configuring-group-policy-for-microsoft-teams-rooms).
* Enable Windows Update.
* Enable PowerShell remoting. You can configure a start-up script to run a simple script: Enable-PSRemoting -Force

You can use PowerShell to perform a number of remote management activities, including getting and setting configuration information. PowerShell remoting must be enabled *before* any PowerShell remote management can take place and should be considered as part of your deployment processes or configured via Group Policy. For more information about these capabilities and enabling them, see [Maintenance and operations](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-operations#remote-management-using-powershell).

**Configuration and deployment**

Planning for configuration and deployment covers the following key areas:

* Account provisioning
* Device software installation
* Device deployment
* Microsoft Teams Rooms application and peripheral device configuration
* Testing
* Asset management

**Account provisioning**

Each Microsoft Teams Rooms device requires a dedicated and unique resource account that must be enabled for both Microsoft Teams or Skype for Business and Exchange. This account must have a room mailbox hosted on Exchange and be enabled as a meeting room in the Teams or Skype for Business deployment. On the Exchange side, calendar processing must be configured so that the device can automatically accept incoming meeting requests. For more information about creating these accounts, see [Configure accounts for Microsoft Teams Rooms](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-configure-accounts).

**Pro Tip** – Make the display names for these accounts descriptive and easy to understand. These are the names that users will see when searching for and adding Microsoft Teams Rooms systems to meetings. Some organizations use the convention *Site*-*Room Name*(*Max Room Capacity*)-RS, so for example Curie—a 12-person conference room in London—might have the display name LON-CURIE(12)-RS.

If your organization has many conference rooms that require multiple, provisioned accounts, you might want to use [Skype Room Systems Accounts Provisioning Scripts](https://myadvisor.fasttrack.microsoft.com/CloudVoice/Downloads?SelectedIDs=5_2_0_4,5_2_0_5) to bulk-provision multiple service accounts in an automated fashion.

|  |  |
| --- | --- |
|  |  |
| Decision points | * Decide the naming convention for your Microsoft Teams Rooms accounts. * Decide whether you’ll create individual accounts or use bulk-provisioning scripts. |
| Next steps | * Start to plan your device deployment. |

**Device software installation**

When planning to deploy Microsoft Teams Rooms, you have a number of options to consider to install the required software. Common scenarios and approaches are described in the following table.

|  |  |
| --- | --- |
| **Scenario** | **Approach** |
| Deploying a small number of Microsoft Teams Rooms devices (<10). | If using Surface Pro–based Microsoft Teams Rooms, follow the [installation instructions for a per-device install](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console). [This handy video walks you through the process.](https://content.cloudguides.com/guides/Configure%20the%20Skype%20Room%20Systems%20console) If using an integrated solution, deploy by using the vendor image and configure settings as required. |
| Deploying between 10 and 50 devices from a single vendor. | Create a WIM-based image, pause after [step 6 in the guidance](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console), and capture a distribution image to be used with your cloning distribution technology. |
| Deploying more than 50 Microsoft Teams Rooms devices, deploying devices from more than one vendor, or requiring organization-specific agents as part of the deployment. | Use a task sequencer–based software build and distribution platform, such as [System Center Configuration Manager](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-scale). |

**Pro Tip** - Each Microsoft Teams Rooms must have a valid and unique machine name on your network. Many monitoring and alerting systems display the machine name as a key identifier, so it’s important to develop a naming convention for Microsoft Teams Rooms deployments that allows support personnel to easily locate the Microsoft Teams Rooms that has been flagged as requiring an action. An example might be using a pattern of MTR-*Site*-*Room Name* (MTR-LON-CURIE).

As part of the deployment, you’ll also need to consider your strategy for managing and configuring the [local accounts](https://docs.microsoft.com/skypeforbusiness/plan-your-deployment/clients-and-devices/skype-room-systems-v2-0#local-accounts) that are created by the Microsoft Teams Rooms application installer.

We provide guidance on how to use the [Microsoft Azure Monitor](https://docs.microsoft.com/skypeforbusiness/plan-your-deployment/clients-and-devices/azure-monitor) to monitor the Microsoft Teams Rooms deployment and report on availability, hardware/software errors, and Microsoft Teams Rooms application version. If you decide to use Microsoft Operations Management Suite, you should install the Operations Management Suite agent as part of the software installation process and configure the workspace connection information for your workspace.

An additional consideration is whether the Microsoft Teams Rooms will be domain-joined. Information about the benefits of domain joining can be found in [Skype Room System domain joining considerations](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/domain-joining-considerations).

|  |  |
| --- | --- |
|  |  |
| Decision points | * Decide the Microsoft Teams Rooms device-naming convention to be used during your deployment. * Decide whether you’ll join Microsoft Teams Rooms devices to your domain, and how to manage and configure local accounts. * Decide whether you’ll use Operations Management Suite to monitor the Microsoft Teams Rooms deployment. * Decide which method you’ll use to deploy the software and agents to the Microsoft Teams Rooms system in preparation for the device deployment. |
| Next steps | * Start to plan your device deployment approach. |

**Device deployment**

After you’ve deployed your software to the Microsoft Teams Rooms units, create your plan to ship the devices and their assigned peripheral devices to your rooms, and then proceed to installation and configuration.

|  |  |
| --- | --- |
|  |  |
| Decision points | * Decide who will manage the site-by-site deployment. * Identify the resources who will install the Microsoft Teams Rooms devices on site and undertake the configuration and testing. |
| Next steps | * Start device testing. |

*Sample deployment table*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Site** | **Room name** | **Room type** | **Microsoft Teams Rooms system** | **Peripheral devices** | **Microsoft Teams Rooms computer name** | **Microsoft Teams Rooms resource account** |
| London HQ | Curie | Medium |  |  |  |  |
| Sydney HQ | Hill | Large |  |  |  |  |

**Microsoft Teams Rooms application and peripheral device configuration**

After each Microsoft Teams Rooms system has been physically deployed and the supported peripheral devices connected, you’ll need to configure the Microsoft Teams Rooms application to assign the Microsoft Teams Rooms resource account and password created earlier, to enable the Microsoft Teams Rooms system to sign in to Microsoft Teams or Skype for Business and Exchange. It's key to leverage certified USB audio and video peripherals linked elsewhere in the document. Not doing so can result in unpredictable behavior.

You can manually configure each Microsoft Teams Rooms system. Alternatively, you can use a centrally stored, per–Microsoft Teams Rooms XML configuration file to manage the application settings and leverage a start-up GPO script to reapply the configuration you want, each time the Microsoft Teams Rooms system boots.

For more information about how to use the XML configuration file, see [Manage a Microsoft Teams Rooms console settings remotely with an XML configuration file](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/xml-config-file).

You can use [remote PowerShell](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-operations#remote-management-using-powershell) to pull the Microsoft Teams Rooms configuration for reporting needs.

|  |  |
| --- | --- |
|  |  |
| Decision points | * Decide whether you’ll manually configure each Microsoft Teams Rooms system or use a central XML file (one per Microsoft Teams Rooms device). |
| Next steps | * Define your remote management approach. |

**Testing**

After the Microsoft Teams Rooms system has been deployed, you should test it. Check that the capabilities listed in [Microsoft Teams Rooms help](https://support.office.com/article/Skype-Room-Systems-version-2-help-e667f40e-5aab-40c1-bd68-611fe0002ba2) are working on the deployed device. We highly recommend that the deployment team verify that the Microsoft Teams Rooms is logging to Microsoft Operations Management Suite (if used). It’s also important that you make a number of test calls and meetings to check quality. For more information, see this [useful deployment checklist](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console#microsoft-teams-rooms-deployment-checklist).

We recommend that as part of the general Teams or Skype for Business rollout, you configure building files for Call Quality Dashboard (CQD), monitor quality trends, and engage in the Quality of Experience Review process. For more information, see the [Quality of Experience Review Guide](https://aka.ms/qerguide).

**Pro Tip** – The [Testing Matrix](https://myadvisor.fasttrack.microsoft.com/CloudVoice/Downloads?SelectedIDs=5_1_0_21) available from [MyAdvisor](https://myadvisor.fasttrack.microsoft.com/) contains a tab with a number of Microsoft Teams Rooms tests that you should review using as part of your testing.

**Asset management**

As part of the deployment, you’ll want to update your asset register with the room name, Microsoft Teams Rooms device name, signed-in Microsoft Teams Rooms resource account, and assigned peripheral devices (and which USB ports they use).

*Sample asset table*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Site** | **Room name** | **Room type** | **Microsoft Teams Rooms serial no.** | **Peripheral devices/ Serial nos./ Ports** | **Microsoft Teams Rooms computer name** | **Microsoft Teams Rooms service account** | **Date deployed** |
| London HQ | Curie | Medium |  |  |  |  |  |
| Sydney HQ | Hill | Large |  | | | | |

**Configure accounts for Microsoft Teams Rooms**

Read this topic to learn about Microsoft Teams Rooms and how it integrates with Exchange and Skype for Business.

This topic introduces how to create accounts used by Microsoft Teams Rooms in Microsoft Exchange and Skype for Business. Deployment instructions for Microsoft Teams Rooms devices is covered in [Configure a Microsoft Teams Rooms console](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console). Your infrastructure will likely fall into one of the following configurations:

* Online deployment: Your organization's environment is deployed entirely on Office 365. For more information, see [Deploy Microsoft Teams Rooms with Office 365](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/with-office-365).
* On-premises deployment: Your organization has servers that it controls, where Active Directory, Exchange, and Skype for Business Server are hosted. For more information, see [Deploy Microsoft Teams Rooms with Skype for Business Server](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/with-skype-for-business-server-2015)
* Hybrid deployments: Your organization has a mix of services, with some hosted on premises and some hosted online through Office 365. With Microsoft Teams Rooms, the following hybrid scenarios are supported:
  + Exchange Online with Skype for Business Server on premises. For more information, see [Deploy Microsoft Teams Rooms with Exchange Online (Hybrid)](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/with-exchange-online).
  + Exchange on premises with Microsoft Teams or Skype for Business Online. For more information, see [Deploy Microsoft Teams Rooms with Exchange on premises (Hybrid)](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/with-exchange-on-premises).

Which configuration you have will affect how you prepare for device setup.

Microsoft Teams Rooms needs to be assigned a "device account" in Active Directory, Exchange, and Skype for Business. The account is used to access its meeting calendar and establish Microsoft Teams or Skype for Business connectivity. People can book this account by scheduling a meeting with it. Microsoft Teams Rooms will be able to join that meeting and provide various features to the meeting attendees.

**Important**

Without a device account, none of these features will work.

Every device account is unique to a single Microsoft Teams Rooms device, and requires some setup:

* The device account must be configured correctly.
* Your infrastructure must be configured to allow Microsoft Teams Rooms to validate the device account, and to reach the appropriate Microsoft services.

**Important**

It is highly recommended that account creation be done well in advance of actual hardware installation. Ideally, account preparation is started two to three weeks before installation. In hybrid environments the account used for Microsoft Teams Rooms must have password sync enabled in AAD Sync because Microsoft Teams Rooms authentication requires 0ffice 365 authentication.

You can think of a device account as the resource account that people recognize as a conference room's or meeting space's account. When you want to schedule a meeting using that conference room, you invite the account to that meeting. In order to use Microsoft Teams Rooms most effectively, you do the same with the device account that's assigned to each one.

If you already have a resource mailbox account set up for the meeting space where you're installing Microsoft Teams Rooms, you can change that resource account into a device account. Once that's done, all you need to do is add the device account to a Microsoft Teams Rooms device. See device account setup examples provided below.

With additional configuration, remote management is possible using Microsoft Azure Monitor as described in [Plan Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-plan), [Deploy Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy), and [Manage Microsoft Teams Rooms devices with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-manage).

**Basic configuration**

These properties represent the minimum configuration for a device account to work with Microsoft Teams Rooms. Your device account may require further setup.

|  |  |
| --- | --- |
| **Property** | **Purpose** |
| Exchange mailbox (Exchange 2013 SP1 or later, or Exchange Online) | Enabling the account with an Exchange mailbox gives the device account the capability to receive and send both mail and meeting requests, and to display a meetings calendar on the Microsoft Teams Rooms device. The Microsoft Teams Rooms mailbox must be a room mailbox. |
| Skype for Business is enabled | Skype for Business must be enabled in order to use various conferencing features, like video calls, IM, and screen-sharing. Both Skype for Business Online and Skype for Business Server are supported. |
| Password-enabled | The device account must be enabled with a password, or it cannot authenticate with either Exchange or Skype for Business Server. |

**Advanced configuration**

While the properties for the basic configuration will allow the device account to be set up in a simple environment, it is possible your environment has other restrictions on directory accounts that must be met in order for Microsoft Teams Rooms to successfully use the device account.

|  |  |
| --- | --- |
| **Property** | **Purpose** |
| Certificate-based authentication | Certificates may be required for both Exchange and Skype for Business Server. To deploy certificates, you can load them when logged in as Admin. |

The easiest way to set up device accounts is to configure them using remote Windows PowerShell. Microsoft provides [SkypeRoomProvisioningScript.ps1](https://go.microsoft.com/fwlink/?linkid=870105), a script that will help create new device accounts, or validate existing resource accounts you have in order to help you turn them into compatible Microsoft Teams Rooms device accounts.

If you prefer to use the Office 365 UI over Windows PowerShell cmdlets, some steps can be performed manually. See [Creating a device account using Office 365](https://docs.microsoft.com/surface-hub/create-a-device-account-using-office-365).

**Deploy Microsoft Teams Rooms with Skype for Business Server**

This topic explains how you add a device account for Microsoft Teams Rooms when you have a single-forest, on-premises deployment.

If you have a single-forest, on-premises deployment with Exchange 2013 SP1 or later and Skype for Business Server 2015 or later, then you can use the provided Windows PowerShell scripts to create device accounts. If you're using a multi-forest deployment, you can use equivalent cmdlets that will produce the same results. Those cmdlets are described in this section.

Before you begin to deploy Microsoft Teams Rooms, be sure you have the right permissions to run the associated cmdlets.

Powershell

Copy

Set-ExecutionPolicy Unrestricted

$org='contoso.com'

$cred=Get-Credential $admin@$org

$sessExchange = New-PSSession -ConfigurationName microsoft.exchange -Credential $cred -AllowRedirection -Authentication Kerberos -ConnectionUri

"http://$strExchangeServer/powershell" -WarningAction SilentlyContinue

$sessLync = New-PSSession -Credential $cred -ConnectionURI "https://$strLyncFQDN/OcsPowershell" -AllowRedirection -WarningAction SilentlyContinue

Import-PSSession $sessExchange

Import-PSSession $sessLync

Note that $strExchangeServer is the fully qualified domain name (FQDN) of your Exchange server, and $strLyncFQDN is the FQDN of your Skype for Business Server deployment.

1. After establishing a session, you'll either create a new mailbox and enable it as a RoomMailboxAccount, or change the settings for an existing room mailbox. This will allow the account to authenticate to Microsoft Teams Rooms.  
    If you're changing an existing resource mailbox:  
    Powershell  
     
    Copy  
    Set-Mailbox -Identity 'PROJECTRIGEL01' -EnableRoomMailboxAccount $true -RoomMailboxPassword (ConvertTo-SecureString -String <password>
2. -AsPlainText -Force)
3. If you're creating a new resource mailbox:  
    Powershell  
     
    Copy  
    New-Mailbox -UserPrincipalName PROJECTRIGEL01@contoso.com -Alias PROJECTRIGEL01 -Name "Project-Rigel-01" -Room
4. -EnableRoomMailboxAccount $true -RoomMailboxPassword (ConvertTo-SecureString -String <password> -AsPlainText -Force)
6. You can set various Exchange properties on the device account to improve the meeting experience for people. You can see which properties need to be set in the Exchange properties section.  
    Powershell  
     
    Copy  
    Set-CalendarProcessing -Identity $acctUpn -AutomateProcessing AutoAccept -AddOrganizerToSubject $false -AllowConflicts $false -DeleteComments
7. $false -DeleteSubject $false -RemovePrivateProperty $false
8. Set-CalendarProcessing -Identity $acctUpn -AddAdditionalResponse $true -AdditionalResponse "This is a Skype Meeting room!"
10. If you decide to have the password not expire, you can set that with Windows PowerShell cmdlets too. See Password management for more information.  
     Powershell  
      
     Copy  
     Set-AdUser $acctUpn -PasswordNeverExpires $true
12. Enable the account in Active Directory so it will authenticate to Microsoft Teams Rooms.  
     Powershell  
      
     Copy  
     Set-AdUser $acctUpn -Enabled $true
14. Enable the device account with Skype for Business Server by enabling your Microsoft Teams Rooms Active Directory account on a Skype for Business Server pool:  
     Powershell  
      
     Copy  
     Enable-CsMeetingRoom -SipAddress sip:PROJECTRIGEL01@contoso.com -DomainController DC-ND-001.contoso.com
15. -RegistrarPool LYNCPool15.contoso.com -Identity PROJECTRIGEL01
16. You'll need to use the Session Initiation Protocol (SIP) address and domain controller for the Project
17. **Optional.** You can also allow Microsoft Teams Rooms to make and receive public switched telephone network (PSTN) phone calls by enabling Enterprise Voice for your account. Enterprise Voice isn't a requirement for Microsoft Teams Rooms, but if you want PSTN dialing functionality for the Microsoft Teams Rooms client, here's how to enable it:  
     Powershell  
      
     Copy  
     Set-CsMeetingRoom PROJECTRIGEL01 -DomainController DC-ND-001.contoso.com -LineURI "tel:+14255550555;ext=50555"
18. Set-CsMeetingRoom -DomainController DC-ND-001.contoso.com -Identity PROJECTRIGEL01 -EnterpriseVoiceEnabled $true
19. Grant-CsVoicePolicy -PolicyName VP1 -Identity PROJECTRIGEL01
20. Grant-CsDialPlan -PolicyName DP1 -Identity PROJECTRIGEL01
21. Again, you'll need to replace the provided domain controller and phone number examples with your own information. The parameter value $true stays the same.

**Sample: room account setup in Exchange and Skype for Business Server on premises**

Powershell

Copy

New-Mailbox -Alias rigel1 -Name "Rigel 1" -Room -EnableRoomMailboxAccount $true -RoomMailboxPassword (ConvertTo-SecureString -String "" -AsPlainText -Force)

-UserPrincipalName rigel1@contoso.com

Set-CalendarProcessing -Identity rigel1 -AutomateProcessing AutoAccept -AddOrganizerToSubject $false -AllowConflicts $false -DeleteComments $false -DeleteSubject $false

-RemovePrivateProperty $false

Set-CalendarProcessing -Identity rigel1 -AddAdditionalResponse $true -AdditionalResponse "This is a Skype Meeting room!"

Enable-CsMeetingRoom -Identity rigel1@contoso.com -RegistrarPool cs3.contoso.com -SipAddressType EmailAddress

Set-CsMeetingRoom -Identity rigel1 -EnterpriseVoiceEnabled $true -LineURI tel:+155555555555

Grant-CsVoicePolicy -PolicyName dk -Identity rigel1

Grant-CsDialPlan -PolicyName e15dp2.contoso.com -Identity rigel1

**Deploy Microsoft Teams Rooms with Exchange Online**

Read this topic for information on how to deploy Microsoft Teams Rooms with Exchange Online and Skype for Business Server on-premises.

If your organization has a mix of services, with some hosted on premises and some hosted online, then your configuration will depend on where each service is hosted. This topic covers hybrid deployments for Microsoft Teams Rooms with Exchange hosted online. Because there are so many different variations in this type of deployment, it's not possible to provide detailed instructions for all of them. The following process will work for many configurations. If the process isn't right for your setup, we recommend that you use Windows PowerShell to achieve the same end result as documented here, and for other deployment options.

The easiest way to set up user accounts is to configure them using remote Windows PowerShell. Microsoft provides [SkypeRoomProvisioningScript.ps1](https://go.microsoft.com/fwlink/?linkid=870105), a script that will help create new user accounts, or validate existing resource accounts you have in order to help you turn them into compatible Microsoft Teams Rooms user accounts. If you prefer, you can follow the steps below to configure accounts your Microsoft Teams Rooms device will use.

**Requirements**

Before you deploy Microsoft Teams Rooms with Exchange Online, be sure you have met the requirements. For more information, see [Microsoft Teams Rooms requirements](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/requirements).

To deploy Microsoft Teams Rooms with Exchange Online, follow the steps below. Be sure you have the right permissions to run the associated cmdlets.

**Create an account and set Exchange properties**

1. Start a remote Windows PowerShell session on a PC and connect to Exchange Online as follows:

Powershell

Copy

Set-ExecutionPolicy Unrestricted

$org='contoso.microsoft.com'

$cred=Get-Credential $admin@$org

$sess= New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $cred -Authentication Basic -AllowRedirection

1. After establishing a session, you'll either create a new mailbox and enable it as a RoomMailboxAccount, or change the settings for an existing room mailbox. This will allow the account to authenticate into Microsoft Teams Rooms.  
    If you're changing an existing resource mailbox:  
    Powershell  
     
    Copy  
    Set-Mailbox -Identity 'PROJECTRIGEL01' -EnableRoomMailboxAccount $true -RoomMailboxPassword (ConvertTo-SecureString -String <password> -AsPlainText -Force)
2. If you're creating a new resource mailbox:  
    Powershell  
     
    Copy  
    New-Mailbox -MicrosoftOnlineServicesID 'PROJECTRIGEL01@contoso.com' -Alias PROJECTRIGEL01 -Name "Project-Rigel-01" -Room -EnableRoomMailboxAccount $true -RoomMailboxPassword (ConvertTo-SecureString -String <password> -AsPlainText -Force)
4. To improve the meeting experience, you'll need to set the Exchange properties on the user account as follows:  
    Powershell  
     
    Copy  
    Set-CalendarProcessing -Identity 'PROJECTRIGEL01@contoso.com' -AutomateProcessing AutoAccept -AddOrganizerToSubject $false -AllowConflicts $false -DeleteComments $false -DeleteSubject $false -RemovePrivateProperty $false
5. Set-CalendarProcessing -Identity 'PROJECTRIGEL01@contoso.com' -AddAdditionalResponse $true -AdditionalResponse "This is a Skype Meeting room!"

**Add an email address for your on-premises domain account**

1. In **Active Directory Users and Computers AD** tool, right-click on the container or Organizational Unit that your Microsoft Teams Rooms accounts will be created in, click **New**, and then click **User**.
2. Type the display name (- Identity ) from the prior cmdlet (Set-Mailbox or New-Mailbox) into the **Full name** box, and the alias into the **User logon name** box. Click **Next**.
3. Type the password for this account. You'll need to retype it for verification. Make sure the **Password never expires** checkbox is the only option selected.  
     **Note** Selecting **Password never expires** is a requirement for Skype for Business Server on Microsoft Teams Rooms. Your domain rules may prohibit passwords that don't expire. If so, you'll need to create an exception for each Microsoft Teams Rooms user account.
4. Click **Finish** to create the account.
5. After you have created the account, run a directory synchronization. This can be accomplished by using [Set-MsolDirSyncConfiguration](https://docs.microsoft.com/powershell/module/msonline/set-msoldirsyncconfiguration?view=azureadps-1.0) in PowerShell. When that is complete, go to the users page and verify that the two accounts created in the previous steps have merged.

**Assign an Office 365 license**

1. First, connect to Azure AD to apply some account settings. You can run this cmdlet to connect. For details about Active Directory, see [Azure ActiveDirectory (MSOnline) 1.0](https://docs.microsoft.com/en-us/powershell/azure/active-directory/overview?view=azureadps-1.0).  
     **Note** [**Azure Active Directory PowerShell 2.0**](https://docs.microsoft.com/en-us/powershell/azure/active-directory/overview?view=azureadps-2.0) is not supported.

PowerShell

Copy

Connect-MsolService -Credential $cred

1. The user account needs to have a valid Office 365 license to ensure that Exchange and Skype for Business Server will work. If you have the license, you need to assign a usage location to your user account—this determines what license SKUs are available for your account. You'll make the assignment in a following step.
2. Next, use Get-MsolAccountSku to retrieve a list of available SKUs for your Office 365 tenant.
3. Once you list out the SKUs, you can add a license using the Set-MsolUserLicense cmdlet. In this case, $strLicense is the SKU code that you see (for example, contoso:STANDARDPACK).

Copy

Set-MsolUser -UserPrincipalName 'PROJECTRIGEL01@contoso.com' -UsageLocation 'US'

Get-MsolAccountSku

Set-MsolUserLicense -UserPrincipalName 'PROJECTRIGEL01@contoso.com' -AddLicenses $strLicense

**Enable the user account with Skype for Business Server**

1. Create a remote Windows PowerShell session from a PC as follows:  
    Powershell  
     
    Copy  
    Import-Module SkypeOnlineConnector
2. $cssess=New-CsOnlineSession -Credential $cred
3. Import-PSSession $cssess -AllowClobber
5. To enable your Microsoft Teams Rooms account for Skype for Business Server, run this command:  
    Powershell  
     
    Copy  
    Enable-CsMeetingRoom -Identity $rm -RegistrarPool 'sippoolbl20a04.infra.lync.com' -SipAddressType EmailAddress
6. If you aren't sure what value to use for the RegistrarPool parameter in your environment, you can get the value from an existing Skype for Business Server user using this command  
    Powershell  
     
    Copy  
    Get-CsOnlineUser -Identity 'alice@contoso.com'| fl \*registrarpool\*

**Assign a Skype for Business Server license to your Microsoft Teams Rooms account**

1. Log in as a tenant administrator, open the Office 365 Administrative Portal, and click on the Admin app.
2. Click on **Users and Groups** and then click **Add users, reset passwords, and more**.
3. Click the Microsoft Teams Rooms account, and then click the pen icon to edit the account information.
4. Click **Licenses**.
5. In **Assign licenses**, select Skype for Business (Plan 2) or Skype for Business (Plan 3), depending on your licensing and Enterprise Voice requirements. You'll have to use a Plan 3 license if you want to use Enterprise Voice on Microsoft Teams Rooms.
6. Click **Save**.

For validation, you should be able to use any Skype for Business client to log in to this account.

**Deploy Microsoft Teams Rooms with Exchange on premises**

Read this topic for information on how to deploy Microsoft Teams Rooms in a hybrid environment with Exchange on premises and Microsoft Teams or Skype for Business Online.

If your organization has a mix of services, with some hosted on premises and some hosted online, then your configuration will depend on where each service is hosted. This topic covers hybrid deployments for Microsoft Teams Rooms with Exchange hosted on premises. Because there are so many different variations in this type of deployment, it's not possible to provide detailed instructions for all of them. The following process will work for many configurations. If the process isn't right for your setup, we recommend that you use Windows PowerShell to achieve the same end result as documented here, and for other deployment options.

Microsoft provides [SkypeRoomProvisioningScript.ps1](https://go.microsoft.com/fwlink/?linkid=870105), a script that will help create new user accounts, or validate existing resource accounts you have in order to help you turn them into compatible Microsoft Teams Rooms user accounts. If you prefer, you can follow the steps below to configure accounts your Microsoft Teams Rooms device will use.

**Requirements**

Before you deploy Microsoft Teams Rooms with Exchange on premises, be sure you have met the requirements. For more information, see [Microsoft Teams Rooms requirements](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/requirements).

If you are deploying Microsoft Teams Rooms with Exchange on premises, you will be using Active Directory administrative tools to add an email address for your on-premises domain account. This account will be synced to Office 365. You will need to:

* Create an account and synchronize the account with Active Directory.
* Enable the remote mailbox and set properties.
* Assign an Office 365 license.
* Enable the device account with Skype for Business Server. To enable the device account your environment will need to meet the following prerequisites:
  + You'll need to have Skype for Business Online (Plan 2) or higher in your Office 365 plan. The plan needs to support conferencing capability.  
    - If you need Enterprise Voice (PSTN telephony) using telephony service providers for Microsoft Teams Rooms you need Skype for Business Online (Plan 3).
    - Your tenant users must have Exchange mailboxes.
    - Your Microsoft Teams Rooms account does require a Skype for Business Online (Plan 2) or Skype for Business Online (Plan 3) license, but it does not require an Exchange Online license.
* Assign a Skype for Business Server license to your Microsoft Teams Rooms account.

**Create an account and synchronize with Active Directory**

1. In the **Active Directory Users and Computers** tool, right-click on the folder or Organizational Unit that your Microsoft Teams Rooms accounts will be created in, click **New**, and then click **User**.
2. Type the display name from the previous cmdlet into the **Full name** box, and the alias into the **User logon name** box. Click **Next**.
3. Type the password for this account. You'll need to retype it for verification. Make sure the **Password never expires** checkbox is the only option selected.  
     **Note** Selecting **Password never expires** is a requirement for Skype for Business Server on Microsoft Teams Rooms. Your domain rules may prohibit passwords that don't expire. If so, you'll need to create an exception for each Microsoft Teams Rooms device account.
4. After you've created the account, run a directory synchronization. When it's complete, go to the users page in your Microsoft 365 admin center and verify that the account created in the previous steps has merged to online.

**Enable the remote mailbox and set propertie**

1. [Open the Exchange Management Shell](https://docs.microsoft.com/powershell/exchange/exchange-server/open-the-exchange-management-shell) or [connect to your Exchange server using remote PowerShell](https://docs.microsoft.com/powershell/exchange/exchange-server/connect-to-exchange-servers-using-remote-powershell).
2. In Exchange PowerShell, crate a mailbox for the account (mailbox-enable the account)by running the following command:  
    Powershell  
     
    Copy  
    Enable-Mailbox PROJECTRIGEL01@contoso.com -Room
3. For detailed syntax and parameter information, see [Enable-Mailbox](https://docs.microsoft.com/powershell/module/exchange/mailboxes/enable-mailbox).
4. In Exchange PowerShell, configure the following settings on the room mailbox to improve the meeting experience:
   * AutomateProcessing: AutoAccept (Meeting organizers receive the room reservation decision directly without human intervention: free = accept; busy = decline.)
   * AddOrganizerToSubject: $false (The meeting organizer is not added to the subject of the meeting request.)
   * DeleteComments: $false (Keep any text in the message body of incoming meeting requests.)
   * DeleteSubject: $false (Keep the subject of incoming meeting requests.)
   * RemovePrivateProperty: $false (Ensures the private flag that was sent by the meeting organizer in the original meeting request remains as specified.)
   * AddAdditionalResponse: $true (The text specified by the AdditionalResponse parameter is added to meeting requests.)
   * AdditionalResponse: "This is a Skype Meeting room!" (The additional text to add to the meeting request.)
5. This example configures these settings on the room mailbox named Project-Rigel-01.  
    PowerShell  
     
    Copy  
    Set-CalendarProcessing -Identity "Project-Rigel-01" -AutomateProcessing AutoAccept -AddOrganizerToSubject $false -DeleteComments $false -DeleteSubject $false -RemovePrivateProperty $false -AddAdditionalResponse $true -AdditionalResponse "This is a Skype Meeting room!"
6. For detailed syntax and parameter information, see [Set-CalendarProcessing](https://docs.microsoft.com/powershell/module/exchange/mailboxes/set-calendarprocessing).

**Assign an Office 365 license**

1. Connect to Azure Active Directory. For details about Active Directory, see [Azure ActiveDirectory (MSOnline) 1.0](https://docs.microsoft.com/en-us/powershell/azure/active-directory/overview?view=azureadps-1.0).  
     **Note** [**Azure Active Directory PowerShell 2.0**](https://docs.microsoft.com/en-us/powershell/azure/active-directory/overview?view=azureadps-2.0) is not supported.
2. The device account needs to have a valid Office 365 license, or Exchange and Microsoft Teams will not work. If you have the license, you need to assign a usage location to your device account—this determines what license SKUs are available for your account. You can use Get-MsolAccountSku to retrieve a list of available SKUs.
3. Next, you can add a license using the Set-MsolUserLicense cmdlet. In this case, $strLicense is the SKU code that you see (for example, contoso:STANDARDPACK).

PowerShell

Copy

Set-MsolUser -UserPrincipalName 'PROJECTRIGEL01@contoso.com' -UsageLocation 'US'

Get-MsolAccountSku

Set-MsolUserLicense -UserPrincipalName 'PROJECTRIGEL01@contoso.com' -AddLicenses $strLicense

For detailed instructions, see [Assign licenses to user accounts with Office 365 PowerShell](https://docs.microsoft.com/office365/enterprise/powershell/assign-licenses-to-user-accounts-with-office-365-powershell#use-the-microsoft-azure-active-directory-module-for-windows-powershell).

**Enable the device account**

Skype for Business Online PowerShell is used to manage services for both Microsoft Teams and Skype for Business Online.

1. Create a remote Windows PowerShell session from a PC as follows:  
    Powershell  
     
    Copy  
    Import-Module SkypeOnlineConnector
2. $cssess=New-CsOnlineSession -Credential $cred
3. Import-PSSession $cssess -AllowClobber
5. To enable your Microsoft Teams Rooms account, run this command:  
    Powershell  
     
    Copy  
    Enable-CsMeetingRoom -Identity $rm -RegistrarPool'sippoolbl20a04.infra.lync.com' -SipAddressType EmailAddress
6. If you aren't sure what value to use for the RegistrarPool parameter in your environment, you can get the value from an existing user using this command:  
    Powershell  
     
    Copy  
    Get-CsOnlineUser -Identity 'alice@contoso.com'| fl \*registrarpool\*

**Assign a license to your Microsoft Teams Rooms account**

1. Log in as a tenant administrator, open the Office 365 Administrative Portal, and click on the Admin app.
2. Click on **Users and Groups** and then click **Add users, reset passwords, and more**.
3. Click the Microsoft Teams Rooms account, and then click the pen icon to edit the account information.
4. Click **Licenses**.
5. In **Assign licenses**, select Skype for Business (Plan 2) or Skype for Business (Plan 3), depending on your licensing and Enterprise Voice requirements. You'll have to use a Plan 3 license if you want to use Enterprise Voice on your Microsoft Teams Rooms.
6. Click **Save**.

For validation, you should be able to use any client to log in to this account.

**Configure a Microsoft Teams Rooms console**

This article describes how to set up the Microsoft Teams Rooms console and its peripherals.

You should only perform these steps if the necessary Microsoft Teams or Skype for Business and Exchange accounts have already been created and tested as described in [Deploy Microsoft Teams Rooms](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2). You will need the hardware and software described in [Microsoft Teams Rooms requirements](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/requirements). This topic contains the following sections:

* [Prepare the installation media](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console#Prep_Media)
* [Install a private CA certificate on the console](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console#Certs)
* [Install Windows 10 and the Microsoft Teams Rooms console app](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console#Reimage)
* [Initial set up of the console](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console#Initial)
* [Microsoft Teams Rooms deployment checklist](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console#Checklist)

**Note**

Microsoft Teams Rooms will only work in a properly configured Microsoft Teams or Skype for Business environment where the device accounts are set up correctly as described in [**Deploy Microsoft Teams Rooms**](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2).

**Prepare the installation media**

Installing the Microsoft Teams Rooms console app requires a USB storage device with at least 32GB of capacity. There should be no other files on the device; any existing files on the USB storage will be lost.

**Note**

Failure to create your Microsoft Teams Rooms installation media according to these instructions will likely result in unexpected behavior.

**Note**

The process below is for creating installation media to image new Microsoft Teams Rooms devices. Existing devices, by default, update automatically from Windows Update and the Windows Store.

1. Download the [CreateSrsMedia.ps1 script](https://go.microsoft.com/fwlink/?linkid=867842).
2. Run the CreateSrsMedia.ps1 script from an elevated prompt on a Windows 10 machine.
3. Follow the script's instructions to create a Microsoft Teams Rooms USB setup disk.

**Tip**

Each time the CreateSrsMedia.ps1 script starts, the screen output will include the name of a log file or transcript for the session. If there are issues with running the script, make sure to have a copy of that transcript available when requesting support.

The CreateSrsMedia.ps1 script automates the following tasks:

1. Download the latest MSI installer for Microsoft Teams Rooms.
2. Determine the build of Windows that the user must supply. The most recently released versions may or may not be tested and supported for use with Microsoft Teams Rooms devices.
3. Download necessary supporting components.
4. Assemble the needed components on the installation media.

A specific version of Windows 10 is required, and this version is only available to volume licensing customers. You can get a copy from the [Volume Licensing Service Center](https://www.microsoft.com/Licensing/servicecenter/).

When finished, remove the USB disk from your computer and proceed to [Install Windows 10 and the Microsoft Teams Rooms console app](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console#Reimage).

**Install Windows 10 and the Microsoft Teams Rooms console app**

You now need to apply the setup media you've created. The target device will run as an appliance and the default user will be set to only run the Microsoft Teams Rooms console app.

1. If the target device will be installed in a dock (e.g., a Surface Pro), disconnect it from the dock.
2. Ensure the target device is not connected to the network.
3. Ensure the target device is connected to AC power.
4. Plug your USB setup disk into the target device.
5. Boot to the USB setup disk. Refer to the manufacturer instructions. If your target device is a Surface Pro, use the following steps to boot to the USB setup disk:  
    a. Press and continue to hold the volume down (-) button.  
    b. Press and release the power button.  
    c. Once Windows setup is booted, release the volume down (-) button.
6. The system will shut down once installation is complete.

After the system has shut down, it is safe to remove the USB setup disk. At this point, you can place the target device in its dock (if using a dock-based product), attach the peripherals needed for your meeting room, and connect to the network. Refer to the manufacturer instructions.

**Selecting a language**

In Creator's Update, you will need to use the ApplyCurrentRegionAndLanguage.ps1 script in scenarios where implicit language selection does not provide the user with the actual application language they want (e.g., they want the console app to come up in French, but it's coming up in English).

**Note**

The following instructions work only for consoles created using Windows Creator's Update. Legacy/in-market systems that have not been set up using media with the new provisioning system will not be able to use these instructions, but should also not suffer from the initial issue that requires this manual intervention (Anniversary Edition let you pick your app language explicitly as part of setup).

**To apply your desired language**

1. Switch to Admin mode.
2. Select the Start menu.
3. Select the gear icon to launch the **Settings** app.
4. Select **Time & language**.
5. Select **Region & language**.
6. Select **Add a language**.
7. Select the language you wish to add.
8. Select the language you just added to the "Languages" list.
9. Select **Set as default**.
10. For any languages you wish to remove:  
     a. Select the language you wish to remove.  
     b. Select **Remove**.
11. Start an elevated command prompt.
12. Run the following command:  
      
      
     Copy  
     powershell -executionpolicy unrestricted c:\Rigel\x64\scripts\provisioning\scriptlaunch.ps1 ApplyCurrentRegionAndLanguage.ps1
14. Restart the system.

Your desired language is now applied to the Microsoft Teams Rooms console.

**Initial set up of the console**

After Windows is installed, the Microsoft Teams Rooms console app will go into its initial Setup process when it is started next or if the /reboot option was chosen.

1. The User Account screen appears. Enter the Skype sign-in address (in user@domain format) of the room account to be used with the console.
2. Enter the password for the room account, and re-enter it to verify.
3. Under "Configure Domain," set the FQDN for the Skype for Business Server. If the Skype for Business SIP domain is different from the Exchange domain of the user, enter the Exchange domain in this field.
4. Click **Next**.
5. Select the indicated devices on the Features screen and click **Next**. The default is to have Auto Screen sharing set to On and Hide meeting names set to Off. The devices to select are:
   * Microphone for Conferencing: the default microphone for this conference room.
   * Speaker for Conferencing: the default speaker for conferencing.
   * Default Speaker: the speaker used for audio from the HDMI ingest.  
      Each item has a drop-down menu of options to select from. You must make a selection for each device.
6. Click **Finish**.

The Microsoft Teams Rooms console app should immediately start signing in to Skype for Business Server with the credentials entered above, and should also begin syncing its calendar with Exchange using those same credentials. For details on using the console app, refer to the [Microsoft Teams Rooms help](https://support.office.com/en-US/article/Skype-Room-Systems-version-2-help-e667f40e-5aab-40c1-bd68-611fe0002ba2).

**Important**

Microsoft Teams Rooms relies on the presence of certified console hardware. Even a correctly created image containing the Microsoft Teams Rooms console app will not boot past the initial setup procedure unless the console hardware is detected. For Surface Pro based solutions, the Surface Pro must be connected to its accompanying dock hardware to pass this check.

**Note**

Some non-English language users may need a physical keyboard connected to the console during initial setup in the event that symbols are not supported on the touch keyboard.

**Install a private CA certificate on the console**

The Microsoft Teams Rooms console needs to trust the certificates used by the servers it connects to. For O365 this is done automatically, since these servers are using public Certificate Authorities and these are automatically trusted by Windows 10. In a case where the Certificate Authority is private, for instance an on-premises deployment with Active Directory and the Windows Certificate Authority, you can add the certificate to the Microsoft Teams Rooms console in a couple of ways:

* You can join the console to Active Directory and that will automatically add the required certificates given the Certificate Authority is published to Active Directory (normal deployment option).
* You can install the certificate manually after the imaging process. Before you do this, you must complete [Initial set up of the console](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console#Initial).

**To manually install the certificate**

1. Download the CA certificate to your computer and save it to "C:\Skype Room Systems\x64\Scripts\Provisioning\CAcertificate.cer".
2. Place the console in admin mode (see [Admin mode and device management](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-operations#AdminMode)).
3. Run the following command:  
     
     
    Copy  
    certutil -addstore -f -enterprise root "C:\Skype Room Systems\x64\Scripts\Provisioning\CAcertificate.cer"

**Join an Active Directory domain (Optional)**

You can join Microsoft Teams Rooms consoles to your domain. Microsoft Teams Rooms consoles should be placed in a separate OU from your PC workstations because many workstation policies are not compatible with Microsoft Teams Rooms. A common example are password enforcement policies that will prevent Microsoft Teams Rooms from starting up automatically. For information about the management of GPO settings, please refer to [Manage Microsoft Teams Rooms](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-operations).

**To join Microsoft Teams Rooms to a domain**

1. Sign into the console from the admin account (see [Admin mode and device management](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-operations#AdminMode)).
2. Launch elevated Powershell command prompt.
3. Enter the following command in Powershell:  
     
     
    Copy  
    Add-Computer -DomainName <Fully qualified domain> -OUPath "OU=<Child OU>, … ,OU=<Top level OU>,DC=<child domain>,…,DC=<top level domain>"

For example, if your fully qualified domain is redmond.corp.microsoft.com and you want your Microsoft Teams Rooms consoles to be in a "Microsoft Teams Rooms" OU that is a child of a "Resources" OU, the command will be:

Copy

Add-Computer -DomainName redmond.corp.microsoft.com -OUPath "OU=Microsoft\_Teams\_Rooms,OU=Resources,DC=redmond,DC=corp,DC=microsoft,DC=com"

If you would like to rename the computer when joining it to a domain, use the -NewName flag followed by the computer's new name.

**Microsoft Teams Rooms deployment checklist**

Use the following checklist while doing a final verification that the console and all its peripherals are fully configured:

**Application settings**

|  |  |
| --- | --- |
|  |  |
| ☐ | Room account name and phone # (if PSTN enabled) are correctly displayed in top right of console screen |
| ☐ | Windows computer name is set correctly (useful for remote administration) |
| ☐ | Administrator account password set and verified |
| ☐ | All firmware updates have been applied |

**Audio/video peripherals**

|  |  |
| --- | --- |
|  |  |
| ☐ | Camera peripheral firmware version is correct (if applicable) |
| ☐ | Camera functional and positioned optimally |
| ☐ | Settings for Playback Default Device and Playback Default Communications Device set to intended audio peripheral |
| ☐ | Settings for Recording Default Communication Device set to the intended audio peripheral |
| ☐ | Audio peripheral firmware version is correct (if applicable) |
| ☐ | Audio input device functional and optimally positioned |
| ☐ | Audio output device functional and optimally positioned |

**Dock**

|  |  |
| --- | --- |
|  |  |
| ☐ | Cables are secure and not pinched |
| ☐ | Audio ingest over HDMI is functional |
| ☐ | Video ingest over HDMI is functional |
| ☐ | Dock can swivel freely |
| ☐ | Display brightness is acceptable for environment |

**Deploy Microsoft Teams Rooms by using System Center Configuration Manager**

This article gives you all the necessary information to create your Microsoft Teams Rooms deployments by using System Center Configuration Manager.

With the easy-to-use methods provided by System Center Configuration Manager, you can deploy the operating system and other applications to multiple target devices.

Use the approach illustrated below to guide you through your Configuration Manager configuration, and customize the sample packages and scripts provided throughout this guidance as needed for your organization.

**Important**

This solution has only been tested with Surface Pro–based deployments. Follow the manufacturer’s guidelines for configurations that aren’t based on Surface Pro.

**Validate prerequisites**

To deploy Microsoft Teams Rooms with Configuration Manager, ensure that you meet the following prerequisites and requirements.

**System Center Configuration Manager requirements**

* System Center Configuration Manager version must be at least 1706 or above. We recommend using 1710 or later. Check out [Support for Windows 10 in System Center Configuration Manager](https://docs.microsoft.com/sccm/core/plan-design/configs/support-for-windows-10#windows-10-as-a-client) to learn about the Windows 10 versions that Configuration Manager supports.
* A supported version of Windows Assessment and Deployment Kit (ADK) for Windows 10 must be installed. See the versions of the [Windows 10 ADK](https://docs.microsoft.com/sccm/core/plan-design/configs/support-for-windows-10#windows-10-adk) that you can use with different versions of Configuration Manager, and ensure that your deployment includes the correct version.
* The site system servers must have been assigned the distribution point role, and the boot images should be enabled for [preboot execution environment (PXE) support](https://docs.microsoft.com/sccm/osd/deploy-use/use-pxe-to-deploy-windows-over-the-network) to enable network-initiated deployments. If PXE support isn’t enabled, you can use [bootable media](https://docs.microsoft.com/sccm/osd/deploy-use/use-bootable-media-to-deploy-windows-over-the-network) for your deployments.
* A network access account must be configured to support new computer (bare metal) deployment scenarios. To learn more about the configuration of a network access account, see [Manage accounts to access content in System Center Configuration Manager](https://docs.microsoft.com/sccm/core/plan-design/hierarchy/manage-accounts-to-access-content#bkmk_NAA).
* We recommend that you enable [multicast support](https://docs.microsoft.com/sccm/osd/deploy-use/use-multicast-to-deploy-windows-over-the-network), if you’re likely to deploy the same Microsoft Teams Rooms image to multiple units at the same time.

**Networking requirements**

* Your network should have a Dynamic Host Configuration Protocol (DHCP) server, configured for automatic IP address distribution to the subnets where Microsoft Teams Rooms units will be deployed.  
    **Note** DHCP lease duration must be set to a value longer than the image deployment duration. Otherwise, the deployment might fail.
* Your network, including switches and virtual LANs (VLANs), should be configured to support PXE. Refer to your network vendor for more information about IP Helper and PXE configuration. Alternatively, you can use [bootable media](https://docs.microsoft.com/sccm/osd/deploy-use/use-bootable-media-to-deploy-windows-over-the-network) for your deployments, if PXE support isn’t enabled.  
    **Note** For Surface Pro devices, booting from the network (PXE boot) is only supported when you use an Ethernet adapter or docking station from Microsoft. Third-party Ethernet adapters don’t support PXE boot with Surface Pro. See [**Ethernet adapters and Surface deployment**](https://docs.microsoft.com/surface/ethernet-adapters-and-surface-device-deployment) for more information.

**Configure System Center Configuration Manager for operating system deployment**

This article assumes you already have a healthy System Center Configuration Manager deployment, and doesn’t detail all the steps required to deploy and configure Configuration Manager from scratch. The [documentation and the configuration guidance](https://docs.microsoft.com/sccm/) on the System Center Configuration Manager is a great resource; we recommend you start with these resources if you haven’t yet deployed Configuration Manager.

Use the following instructions to verify that the operating system deployment (OSD) features are configured properly.

**Validate and upgrade Configuration Manager**

1. In the Configuration Manager console, go to **Administration** > **Updates and Servicing**.
2. Check the installed build and applicable updates that haven’t been installed yet.
3. Review [Support for Windows 10 in System Center Configuration Manager](https://docs.microsoft.com/sccm/core/plan-design/configs/support-for-windows-10#windows-10-as-a-client); if you need to upgrade your deployment, select the update you want to install, and then select **Download**.
4. After the download is complete, select the update, and then select **Install Update Pack**.

**Configure distribution points to support PXE and multicast**

1. In the Configuration Manager console, go to **Administration** > **Distribution Points**.
2. Select the distribution point server that will serve the Microsoft Teams Rooms deployment, and then select **Properties**.
3. Select the **PXE** tab, and ensure that the following settings are enabled:
   * Enable PXE support for clients
   * Allow this distribution point to respond to incoming PXE requests
   * Enable unknown computer support
4. *Optional:* To enable multicast support, select the **Multicast** tab, and ensure that the following settings are enabled:
   * Enable multicast to simultaneously send data to multiple clients
   * Configure the UDP port range as per your network team’s recommendation

**Configure the Network Access Account**

1. In the Configuration Manager console, go to **Administration** > **Site Configuration** > **Sites**, and then select the site.
2. In the **Settings** group, select **Configure Site Components** > **Software Distribution**.
3. Select the **Network Access Account** tab. Set up one or more accounts, and then select **OK**.

**Note**

The accounts don’t need any special rights, except for the **Access this computer from the network** right on the distribution point server. A generic domain user account will be appropriate. For more information, see [**Manage accounts to access content in System Center Configuration Manager**](https://docs.microsoft.com/sccm/core/plan-design/hierarchy/manage-accounts-to-access-content#bkmk_NAA).

**Configure a boot image**

1. In the Configuration Manager console, go to **Software Library** > **Operating System** > **Boot Images**.
2. Select **Boot image (x64)**, and then select **Properties**.
3. Select the **Data Source** tab, and enable **Deploy this boot image from the PXE-enabled distribution point**.
4. Select the **Optional Components** tab to install required components:
   1. Select the star icon, and search for **HTML (WinPE-HTA)**
   2. Select **OK** to add HTML application support in to the boot image.
5. *Optional:* To customize the deployment experience, select the **Customization** tab.
   1. Enable **command support (testing only)** if you want to have access to a command prompt during the deployment. When this is enabled, you can start a command prompt by selecting **F8** at any time during the deployment.
   2. You can also specify a custom background image to be displayed during the deployment. To set an image, enable **Specify the custom background image file (UNC path** and select your background.
6. When asked, select **Yes** and distribute the updated boot image to your distribution points.

For more information, see [Manage boot images with System Center Configuration Manager](https://docs.microsoft.com/sccm/osd/get-started/manage-boot-images).

**Note**

You can create a bootable USB media to initiate Configuration Manager task sequence–based deployments for environments that have no PXE support. The bootable media contains only the boot image, optional prestart commands and their required files, and Configuration Manager binaries to support booting into Windows PE and connecting to Configuration Manager for the rest of the deployment process. For more information, see [**How to Create Bootable Media**](https://docs.microsoft.com/sccm/osd/deploy-use/create-bootable-media#BKMK_CreateBootableMedia).

**Create Configuration Manager packages**

Configuration Manager requires a number of packages to deploy and configure the Microsoft Teams Rooms units.

You need to create and configure the following packages, and then distribute them to the Configuration Manager site systems that have been assigned the distribution point server role.

|  |  |  |
| --- | --- | --- |
| **Package name** | **Type** | **Description** |
| SRS v2 - SRS Application Package | Software package | Package for the Microsoft Teams Rooms deployment kit |
| SRS v2 - Sysprep Package | Software package | Package for the custom Unattended.xml to configure Microsoft Teams Rooms units |
| SRS v2 - Set-SRSComputerName Package | Software package | Package for the HTML application (HTA) to assign a computer name during the deployment |
| SRS v2 - Configure SRS Setup | Software package | Package to configure deployment of the Microsoft Teams Rooms app |
| SRS v2 - OS Updates Package | Software package | Package to deploy mandatory operating system updates |
| SRS v2 - Root Certificate Package | Software package | Optional - Package to deploy the root certificate (not required for domain-joined units) |
| SRS v2 - Microsoft Monitoring Agent Package | Software package | Optional - Package to deploy and configure the Microsoft Operations Management Suite agent |
| SRS v2 - WinPE Background Package | Software package | Package for the custom background image to use with boot images |
| Windows 10 Enterprise | Operating system image | Package for the operating system installation file (install.wim) |
| Surface Pro | Driver package | Package for the device drivers and firmware for Microsoft Surface Pro |
| Surface Pro 4 | Driver package | Package for the device drivers and firmware for Microsoft Surface Pro 4 |

For more information, see [Packages and programs in System Center Configuration Manager](https://docs.microsoft.com/sccm/apps/deploy-use/packages-and-programs).

**Create folders for the package source files**

Configuration Manager requires package source files to be organized in a specific folder structure when they’re first created and when they’re updated.

Create the following folder structure on the System Center Configuration Manager central administration site or primary site, or on a server share you’re using to host package source files:

* SRS v2 - Microsoft Monitoring Agent Package
* SRS v2 - OS Updates Package
* SRS v2 - Root Certificate Package
* SRS v2 - Set-SRSComputerName Package
* SRS v2 - SRS Application Package
* SRS v2 - Configure SRS Setup
* SRS v2 - Sysprep Package
* Drivers
  + Surface Pro
  + Surface Pro 4
* Operating Systems
  + Windows 10 Enterprise

**Tip**

You may also [**download**](https://github.com/MicrosoftDocs/OfficeDocs-SkypeForBusiness/blob/live/Skype/SfbOnline/downloads/Skype-Room-Systems-v2/SRS-v2-Configuration-Manager-Files.zip?raw=true) and use the zip file that includes the folder structure for the packages, the scripts that you need to use, and the task sequence template, that you need to import.

**Create the Monitoring agent package**

1. Download the Monitoring agent from <https://go.microsoft.com/fwlink/?LinkId=828603>.
2. Extract the package into the **SRS v2 - Microsoft Monitoring Agent Package** folder by opening a Command Prompt window and entering **MMASetup-AMD64.exe /C:** at the command prompt.
3. In the Configuration Manager console, go to **Software Library** > **Application Management**> **Packages**, and then select **Create Package**.
4. Enter the following information to create the package:
   * Name**: SRS v2 - Microsoft Monitoring Agent Package**
   * Manufacturer**: Microsoft Corporation**
   * Version**: 8.1.11081.0** (enter the version of the downloaded installation file)
   * Select the **This package contains source files** check box, enter the path to the **SRS v2 - Microsoft Monitoring Agent Package** folder, and then select **Next**.
5. Select **Do not create a program**, and then select **Next**.
6. Review the **Confirm the settings** page, and then select **Next**.
7. Select **Close**.

**Create the operating system updates package**

1. In the **SRS v2 - OS Updates Package** folder, create a new PowerShell script named **Install-SRSv2-OS-Updates.ps1**.
2. Copy the script below into the **Install-SRSv2-OS-Updates.ps1** script. Alternatively, you can download the Install-SRSv2-OS-Updates.ps1 script from [here](https://github.com/MicrosoftDocs/OfficeDocs-SkypeForBusiness/blob/live/Skype/SfbOnline/downloads/Skype-Room-Systems-v2/SRS-v2-Configuration-Manager-Files.zip?raw=true).  
     
     
    Copy  
    # Install-SRSv2-OS-Updates.ps1
3. $strPath = split-path -parent $MyInvocation.MyCommand.Definition
4. $total = gci $strPath \*.msu | measure | Select-Object -expand Count
5. $i = 0
6. gci $strPath \*.msu | ForEach-Object {
7. $i++
8. WUSA ""$\_.FullName /quiet /norestart""
9. Write-Progress -activity "Applying Mandatory Updates" -status "Installing
10. $\_ .. $i of $total" -percentComplete (($i / $total) \* 100)
11. Wait-Process -name wusa
12. }
14. Download the mandatory Windows Update packages into the same folder.  
      **Note** At the time this article was published, only [**KB4056892**](http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows10.0-kb4056892-x64_a41a378cf9ae609152b505c40e691ca1228e28ea.msu) was required. Check [**Configure a Microsoft Teams Rooms console**](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console), to see whether any other updates are required.
15. In the Configuration Manager console, go to **Software Library** > **Application Management**> **Packages**, and then select **Create Package**.
16. Enter the following information to create the package:
    * Name: **SRS v2 – OS Updates Package**
    * Manufacturer: **Microsoft Corporation**
    * Version: **1.0.0**
    * Select the **This package contains source files** check box, enter the path to the **SRS v2 - OS Updates Package** folder, and then select **Next**.
17. Select **Do not create a program**, and then select **Next**.
18. Review the **Confirm the settings** page, and then select **Next**.
19. Select **Close**.

**Create the root certificate package (optional)**

You create this package to distribute the root certificate for devices that won’t be joined to an Active Directory domain. Create this package only if both the following conditions apply:

* Your deployment includes on-premises Lync or Skype for Business Server.
* Microsoft Teams Rooms units are configured to work in a workgroup instead of a domain member.

1. Copy the root certificate into the **SRS v2 – Root Certificate Package** folder.
2. In the Configuration Manager console, go to **Software Library** > **Application Management**> **Packages**, and then select **Create Package**.
3. Enter the following information to create the package:
   * Name: **SRS v2 – Root Certificate Package**
   * Manufacturer: *Your organization’s name*
   * Version: **1.0.0**
   * Select the **This package contains source files** check box, enter the path to the **SRS v2 – Root Certificate Package** folder, and then select **Next**.
4. Select **Do not create a program**, and then select **Next**.
5. Review the **Confirm the settings** page, and then select **Next**.
6. Select **Close**.

**Create the Microsoft Teams Rooms deployment kit package**

1. Download the latest version of the **Microsoft Teams Rooms deployment kit** from <https://go.microsoft.com/fwlink/?linkid=851168>, and install it to a workstation.
2. Copy the content from **C:\Program Files (x86)\Skype Room System Deployment Kit** to the **SRS v2 - SRS Application Package** folder.
3. In the Configuration Manager console, go to **Software Library** > **Application Management**> **Packages**, and then select **Create Package**.
4. Enter the following information to create the package:
   * Name: **SRS v2 – SRS Application Package**
   * Manufacturer: **Microsoft Corporation**
   * Version: **3.1.104.0** (enter the version of the downloaded installation file)
   * Select the **This package contains source files** check box, enter the path to the **SRS v2 – SRS Application Package** folder, and then select **Next**.
5. Select **Do not create a program**, and then select **Next**.
6. Review the **Confirm the settings** page, and then select **Next**.
7. Select **Close**.

**Create the computer name assignment package**

1. In the **SRS v2 - Set-SRSComputerName Package** folder, create a new HTML application named **Set-SRSComputerName.hta** .
2. Copy the following script into the **Set-SRSComputerName.hta** file. Alternatively, you can download the Set-SRSComputerName.hta file from [here](https://github.com/MicrosoftDocs/OfficeDocs-SkypeForBusiness/blob/live/Skype/SfbOnline/downloads/Skype-Room-Systems-v2/SRS-v2-Configuration-Manager-Files.zip?raw=true).  
     
     
    Copy  
    <!DOCTYPE HTML>
3. <html>
4. <head>
5. <title>Set SRS Computer Name</title>
6. <HTA:APPLICATION
7. APPLICATIONNAME="Set SRS Computer Name"
8. ID="SetSRSComputerName"
9. VERSION="1.0"
10. SCROLL="no"
11. SINGLEINSTANCE="yes"
12. WINDOWSTATE="maximize"
13. MaximizeButton="no"
14. MinimizeButton="no"
15. SysMenu="no"
16. ShowInTaskbar="no"
17. Caption="no"
18. />
19. <style type="text/css">
20. body {
21. background-color: #fdfeff;
22. color: darkblue;
23. font-family: Calibri;
24. font-size: 12pt;
25. margin: 4em 3em;
26. }
27. </style>
28. </head>
29. <script language="VBScript">
30. Public strNewComputerName
31. Sub GenerateComputerName()
32. strComputer = "."
33. Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
34. Set colItems = objWMIService.ExecQuery("Select \* from Win32\_BIOS",,48)
35. For Each objItem in colItems
36. strSerialNumber = objItem.SerialNumber
37. Next
38. strNewComputerName = "SRS-" & right(replace(strSerialNumber, "-","") ,10)
39. TextArea1.innerHTML = "The serial number of the device: " & strSerialNumber
40. strHTMLText = strHTMLText & "<br> Computer name to be assigned: <font color = red>" & strNewComputerName & "</font>"
41. strHTMLText = strHTMLText & "<br><br> Click Accept to use this as the computer name and continue deployment, or Change to set a new name."
42. strHTMLText = strHTMLText & "<p><input type=""button"" value=""Accept"" name = ""Accept\_Button"" onclick=""SetComputerName"" />"
43. strHTMLText = strHTMLText & " <input type=""button"" value=""Change"" name = ""Change\_Button"" onclick=""ChangeComputerName"" />"
44. TextArea2.innerHTML = strHTMLText
45. End Sub
46. Sub SetComputerName()
47. dim result
48. result = MsgBox("Computer Name to be assigned: " & strNewComputerName &vbcrlf & "Are you sure you want to continue?", 36)
49. If (result = vbYes) then
50. SET env = CreateObject("Microsoft.SMS.TSEnvironment")
51. env("OSDComputerName") = strNewComputerName
52. self.close
53. elseif (result = vbNo) then
54. Window\_OnLoad
55. End If
56. End Sub
57. Sub UpdateComputerName()
58. strNewComputerName = newcomputername.value
59. if len(trim(strNewComputerName)) = 0 then
60. MsgBox "Computer name cannot be empty." &vbcrlf & "Update and try again.",16
61. exit sub
62. end if
63. SetComputerName
64. End Sub
65. Sub ChangeComputerName()
66. TextArea2.innerHTML = "<p>Type the new computer name and click Accept: <input type=""text"" name=""newcomputername"" value =" & strNewComputerName & " />"
67. TextArea2.innerHTML = TextArea2.innerHTML & "<br><input type=""button"" value=""Update"" name = ""Update\_Button"" onclick=""UpdateComputerName"" />"
68. End Sub
69. Sub Window\_OnLoad
70. Set oTSProgressUI = CreateObject("Microsoft.SMS.TsProgressUI")
71. oTSProgressUI.CloseProgressDialog
72. GenerateComputerName
73. End Sub
74. </script>
75. <body>
76. <span id = "TextArea1"></span>
77. <span id = "TextArea2">
78. </span>
79. </body>
80. </html>
82. In the Configuration Manager console, go to **Software Library** > **Application Management**> **Packages**, and then select **Create Package**.
83. Enter the following information to create the package:
    * Name: **SRS v2 - Set-SRSComputerName Package**
    * Manufacturer: **Microsoft Corporation**
    * Version: **1.0.0**
    * Select the **This package contains source files** check box, enter the path to the **SRS v2 - Set-SRSComputerName Package** folder, and then select **Next**.
84. Select **Do not create a program**, and then select **Next**.
85. Review the **Confirm the settings** page, and then select **Next**.
86. Select **Close**.

**Create the Sysprep package**

1. In the **SRS v2 – Sysprep Package** folder, create a new XML file named **Unattend.xml** .
2. Copy the following text into the **Unattend.xml** file. Alternatively, you can download the Unattend.xml file from [here](https://github.com/MicrosoftDocs/OfficeDocs-SkypeForBusiness/blob/live/Skype/SfbOnline/downloads/Skype-Room-Systems-v2/SRS-v2-Configuration-Manager-Files.zip?raw=true).  
     
     
    Copy  
    <?xml version="1.0" encoding="utf-8"?>
3. <unattend xmlns="urn:schemas-microsoft-com:unattend">
4. <settings pass="specialize">
5. <component name="Microsoft-Windows-Embedded-BootExp" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="NonSxS" xmlns:wcm="https://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
6. <DisableBootMenu>1</DisableBootMenu>
7. <DisplayDisabled>1</DisplayDisabled>
8. </component>
9. <component name="Microsoft-Windows-powercpl" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="https://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
10. <PreferredPlan>8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c</PreferredPlan>
11. </component>
12. </settings>
13. <settings pass="oobeSystem">
14. <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="https://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
15. <OOBE>
16. <HideEULAPage>true</HideEULAPage>
17. <HideLocalAccountScreen>true</HideLocalAccountScreen>
18. <HideOEMRegistrationScreen>true</HideOEMRegistrationScreen>
19. <HideOnlineAccountScreens>true</HideOnlineAccountScreens>
20. <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
21. <SkipMachineOOBE>true</SkipMachineOOBE>
22. <SkipUserOOBE>true</SkipUserOOBE>
23. <ProtectYourPC>1</ProtectYourPC>
24. </OOBE>
25. <AutoLogon>
26. <Enabled>true</Enabled>
27. <Username>Skype</Username>
28. <Password>
29. <Value>UABhAHMAcwB3AG8AcgBkAA==</Value>
30. <PlainText>false</PlainText>
31. </Password>
32. </AutoLogon>
33. <UserAccounts>
34. <LocalAccounts>
35. <LocalAccount wcm:action="add">
36. <Password>
37. <Value>cwBmAGIAUABhAHMAcwB3AG8AcgBkAA==</Value>
38. <PlainText>false</PlainText>
39. </Password>
40. <Name>Admin</Name>
41. <Group>Administrators</Group>
42. <DisplayName>Administrator</DisplayName>
43. <Description>Administrator</Description>
44. </LocalAccount>
45. </LocalAccounts>
46. </UserAccounts>
47. </component>
48. </settings>
49. <cpi:offlineImage cpi:source="wim:h:/install.wim#Windows 10 Enterprise" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
50. </unattend>
52. In the Configuration Manager console, go to **Software Library** > **Application Management**> **Packages**, and then select **Create Package**.
53. Enter the following information to create the package:
    * Name: **SRS v2 - Sysprep Package**
    * Manufacturer: **Microsoft Corporation**
    * Version: **1.0.0**
    * Select the **This package contains source files** check box, enter the path to the **SRS v2 – Sysprep Package** folder, and then select **Next**.
54. Select **Do not create a program**, and then select **Next**.
55. Review the **Confirm the settings** page, and then select **Next**.
56. Select **Close**.

**Create the Windows 10 Enterprise package**

1. Obtain a Windows 10 Enterprise x64 media, and copy the **install.wim** file to the **Operating Systems\Windows 10 Enterprise** folder.
2. In the Configuration Manager console, go to **Software Library** > **Operating Systems** > **Operating System Images**, and then select **Add Operating System Image**.
3. Specify the path to the **install.wim** file you just copied, and then select **Next**.
4. Update the **Version** field to match the build number of the Windows 10 Enterprise image, and then select **Next**.
5. Review the **Details** page, and then select **Next**.
6. Select **Close**.

For more information, see [Manage operating system images with System Center Configuration Manager](https://docs.microsoft.com/sccm/osd/get-started/manage-operating-system-images).

**Create Surface Pro device driver packages**

Microsoft Teams Rooms is supported for both Surface Pro and Surface Pro 4. You need to create a driver package for each Surface Pro model you have in your environment.

**Important**

The drivers must be compatible with the Windows 10 Enterprise build and the Microsoft Teams Rooms deployment kit version. For more information, see [**Download the latest firmware and drivers for Surface devices**](https://docs.microsoft.com/surface/deploy-the-latest-firmware-and-drivers-for-surface-devices) and [**Configure a console**](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console).

1. Download the latest drivers and firmware.
   * For Surface Pro: <https://www.microsoft.com/download/details.aspx?id=55484>
   * For Surface Pro 4: <https://www.microsoft.com/download/details.aspx?id=49498>
2. Extract the downloaded driver and firmware. Open a Command Prompt window and at the command prompt, enter one of the following commands:
   * msiexec /a C:\SurfacePro\_Win10.msi /passive TARGETDIR="C:\\_Sources\\Drivers\Surface Pro"
   * msiexec /a C:\SurfacePro4\_Win10.msi /passive TARGETDIR="C:\\_Sources\\Drivers\Surface Pro 4"
3. In the Configuration Manager console, go to **Software Library** > **Operating Systems** > **Drivers**, and then select **Import Driver**.
4. Select **Import all drivers in the following network path (UNC)**, select the source folder (for example, C:\\_Sources\Drivers\Surface Pro), and then select **Next**.
5. On the **Specify the details for the imported drivers** page, select all the listed drivers, and then select **Enable these drivers and allow computers to install them**.
6. Select **Categories**, create a new category that matches the Surface model, select **OK**, and then select **Next**.
7. Select **New Package**.
8. Specify the package name that matches the Surface Pro model, enter a folder path to store the driver package files in, select **OK**, and then select **Next**.
9. On the **boot images** page, ensure that no boot images are selected, and then select **Next**.
10. Select **Close**.
11. Go to **Software Library** > **Operating Systems** > **Drivers**, select **Folder > Create Folder**, and enter a folder name that matches the Surface Pro model that you just imported the drivers for.
12. Move all the imported drivers to the newly created folder for easier navigation and operation.

**Note**

Repeat the same steps for other Surface Pro models you might have. For more information, see [**Manage drivers in System Center Configuration Manager**](https://docs.microsoft.com/sccm/osd/get-started/manage-drivers).

**Create Microsoft Teams Rooms Configuration Package**

1. In the Configuration Manager console, go to **Software Library** > **Application Management**> **Packages**, and then select **Create Package**.
2. Enter the following information to create the package:
   * Name: **SRS v2 - Configure SRS Setup Package**
   * Manufacturer: **Microsoft Corporation**
   * Version: **1.0.0**
   * Select the **This package contains source files** check box, enter the path to the **SRS v2 - Configure SRS Setup** folder, and then select **Next**.
3. Select **Do not create a program**, and then select **Next**.
4. Review the **Confirm the settings** page, and then select **Next**.
5. Select **Close**.

**Distribute Configuration Manager packages**

All the packages must be distributed to the servers that have been assigned the distribution point role in the Configuration Manager hierarchy. Follow the instructions below to initiate package distribution.

1. Distribute software packages.
   1. In the Configuration Manager console, go to **Software Library** > **Application Management** > **Packages**. Select all the software packages you want to distribute, and then select **Distribute Content**.
   2. Review the list of packages, and then select **Next**.
   3. Add all the distribution point servers (or distribution point groups, depending on your Configuration Manager hierarchy) to the list, and then select **Next**.
   4. Select **Next**, and then select **Close**.
2. Distribute driver packages.
   1. In the Configuration Manager console, go to **Software Library** > **Operating Systems** > **Driver Packages**. Select all the driver packages you want to distribute, and then select **Distribute Content**.
   2. Review the list of packages, and then select **Next**.
   3. Add all the distribution point servers (or distribution point groups, depending on your Configuration Manager hierarchy) to the list, and then select **Next**.
   4. Select **Next**, and then select **Close**.
3. Distribute operating system packages.
   1. In the Configuration Manager console, go to **Software Library** > **Operating Systems** > **Operating System Images**. Select all the operating system images you want to distribute, and then select **Distribute Content**.
   2. Review the list of packages, and then select **Next**.
   3. Add all the distribution point servers (or distribution point groups, depending on your Configuration Manager hierarchy) to the list, and then select **Next**.
   4. Select **Next**, and then select **Close**.

**Note**

Package distribution might take some time, depending on the package size, Configuration Manager hierarchy, number of distribution point servers, and the bandwidth available in your network.

All the packages must be distributed before you can start deploying a Microsoft Teams Rooms unit.

You can review the status of your package distribution in the Configuration Manager console by going to **Monitoring** > **Distribution Status** > **Content Status**.

**Configuration Manager task sequences**

You use task sequences with System Center Configuration Manager to automate the steps for deploying an operating system image to a destination computer. To deploy a Microsoft Teams Rooms unit in an automated fashion, you create a task sequence that references the boot image used to start the destination Microsoft Teams Rooms computer, the Windows 10 Enterprise operating system image that you want to install, and any other additional content, such as other applications or software updates.

**Import the sample task sequence**

You can download and easily import a sample task sequence and customize it to meet your needs.

1. [**Download**](https://github.com/MicrosoftDocs/OfficeDocs-SkypeForBusiness/blob/live/Skype/SfbOnline/downloads/Skype-Room-Systems-v2/SRS-v2-Configuration-Manager-Files.zip?raw=true) the sample task sequence, and copy the downloaded zip file to a shared location.
2. In the Configuration Manager console, go to **Software Library** > **Operating Systems** > **Task Sequences**, and then select **Import Task Sequence**.
3. Select **Browse**, go to the shared folder location you used in step 1, select the **Microsoft Teams Rooms Deployment (EN-US).zip** file, and then select **Next**.
4. Set **Action** to **Create New**, and then select **Next**.
5. Confirm the settings, and then select **Next**.
6. Select **Close**.

**Validate that the reference packages are correctly linked to each task sequence step.**

1. Select the imported task sequence, and then select **Edit**.  
    The Task Sequence Editor opens and displays each sequential step that you need to deploy and configure a Microsoft Teams Rooms unit.
2. Walk through each step and complete the recommended updates:
   1. **Restart in Windows PE**: This step restarts and then boots the computer into Windows PXE. No changes are required for this step.
   2. **Partition Disk 0 – UEFI**: This step wipes the disk configuration and creates partitions based on the configured settings. We recommend that you not make any changes to this step.
   3. **Set SRS Computer Name**: This step includes an HTML application to provide a UI to set a computer name for the Microsoft Teams Rooms unit during the deployment.
      * This is an optional step, but it can only be disabled if you want to manage computer naming through an alternate process.
      * Verify that the **SRS v2 - Set-SRSComputerName** package is selected. If it isn’t, browse to the package and select it.
   4. **Apply Operating System**: This step specifies the operating system image to be deployed and the unattended Sysprep answer file to use.
      * Verify that the correct Windows 10 Enterprise operating system image file is selected.
      * Verify that **Use an unattended or Sysprep answer file for a custom installation** is enabled, and the **SRS v2 - Sysprep Package** is selected. Also ensure that **File Name**is set to **unattend.xml**.
   5. **Apply Windows Settings**: This step gathers information about the Windows installation.
      * Provide licensing and registration information including the product key, local administrator account password, and time zone (depending on your needs).
   6. **Apply Network Settings**: This step allows you to specify a workgroup or Active Directory domain name and organizational unit.  
        **Note** See [**Skype Room System domain joining considerations**](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/domain-joining-considerations) for recommended actions you need to take in deploying Microsoft Teams Rooms units as members of an Actve Directory domain.
   7. **Apply Drivers:** This step and its sub-steps are used to deploy applicable device drivers and firmware based on the Surface Pro model you have. Update each step to specify the relevant driver package associated with this deployment.
      * Each driver package is configured to leverage Windows Management Instrumentation (WMI) filters to deploy relevant drivers and firmware based on the Surface Pro make and model.
      * We highly recommend that you not alter the configuration of these drivers, otherwise deployment might fail.
   8. **Set up Windows and Configuration Manager**: This step deploys and configures the Configuration Manager client. Update this step to specify the built-in Configuration Manager Client Package.
   9. **Install Root Certificate**: This step distributes the root certificate for non–domain-joined devices, and therefore is optional and disabled by default.
      * Enable this step if you need to deploy a root certificate to the Microsoft Teams Rooms units.
      * If you do need to perform this step, verify that the **SRS v2 – Root Certificate Package** and **Disable 64-bit file system redirection** are selected.
   10. **Install and Configure Monitoring Agent**: This step installs the 64-bit version of the Microsoft Azure Monitor agent and configures the agent to connect to your Log Analytics workspace.
       * This step is disabled by default. Enable this step only if you’re going to use the Monitoring Agent to monitor the health of your Microsoft Teams Rooms units.
       * Edit this step and update the command-line parameters to specify your **Workspace ID** and **Workspace Key**.
       * See [Configure test devices for Azure Monitoring](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#configure-test-devices-for-azure-monitoring) for more information about obtaining the Operations Management Suite Workspace ID and the primary key.
       * Verify that the **SRS v2 – Microsoft Monitoring Agent Package** and **Disable 64-bit file system redirection** are selected.
       * For more information about monitoring the health of your Microsoft Teams Rooms deployment, see [Plan Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-plan), [Deploy Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy) and [Manage Microsoft Teams Rooms devices with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-manage).
   11. **Copy SRS v2 Configuration Files**: This step copies the required setup and configuration files from the Microsoft Teams Rooms deployment kit to the local hard drive. No customization is required for this step.
       * Verify that the **SRS v2 – SRS Application Package** and **Disable 64-bit file system redirection** are selected.
   12. **Install-SRSv2-OS-Updates**: This step deploys any mandatory operating system updates required with the Microsoft Teams Rooms deployment. Do the following:
       * Check [Configure a Microsoft Teams Rooms console](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console) to see which updates are required.
       * Verify that your **SRS v2 – OS Updates Package** includes all the required updates.
       * Verify that the **SRS v2 – OS Updates Package** is selected.
       * Verify that the PowerShell execution policy is set to **Bypass**.
   13. **Restart Computer**: This step reboots the computer after the mandatory operating system updates are installed. No customization is required for this step.
   14. **Configure Windows Components**: This step configures the required Windows features. No customization is required for this step.
   15. **Restart Computer**: This step reboots the computer after the Windows features are configured. No customization is required for this step.
   16. **Add Local Skype User**: This step creates the local Skype account used to automatically sign in to Windows and start the Microsoft Teams Rooms application. This step doesn’t have any software package associated with it, and no customization is required for it.
   17. **Set up and configure SRS application**: This step configures the Microsoft Teams Rooms application installation for the next boot of the operating system.
       * Verify that the **SRS v2 – Configure SRS Setup Package** and **Disable 64-bit file system redirection** are selected.

**Important**

It is very important that the task sequence steps must be in the provided order. Modifying the order of steps, or configuring additional steps might break the deployment.

**Set up and configure SRS application** step must be the last step in the task sequence, otherwise the deployment might fail.

**Create deployment for the task sequence**

1. Select the task sequence, and then select **Deploy**.
2. Select **Browse** to select target collection for deployment.
3. Select **All Unknown Computers** and then select **OK**.
4. Select **Next**.
5. Select **Available** on the **Purpose** drop down list.
6. Select **Only Media and PXE** in the **Make available to the following** list, and then select **Next**.  
     **Warning** It is very important that **Purpose** is set to **Available**. Make sure that the **Purpose** is **NOT**set to **Required**. Also make sure that you select **Only Media and PXE** in the **Make available to the following**.  
    Setting these values to something else might cause all computers to get the Microsoft Teams Rooms deployment image when booted.
7. Do not specify any schedule and select **Next**.
8. Do not change anything within the **User Experience** section and select **Next**.
9. Do not change anything within the **Alerts** section and select **Next**.
10. Do not change anything within the **Distribution Points** section and select **Next**.
11. Confirm the settings and then select **Next**.
12. Select **Close**.

**Validate and troubleshoot the solution**

After you’ve completed the System Center Configuration Manager task sequences, you’ll need to perform a test run to validate that the task sequence can deploy and configure Microsoft Teams Rooms units.

1. Connect the test device to the wired network by using one of the supported Ethernet adapters or using the Surface dock. If PXE boot functionality hasn’t been configured for your environment, you can use the boot image on the USB flash drive [that you created earlier](https://docs.microsoft.com/sccm/osd/deploy-use/create-bootable-media) to boot from USB and connect to Configuration Manager.
2. Access the firmware and initiate PXE boot:
   1. Ensure the Surface device is powered off.
   2. Press and hold the **Volume Up** button.
   3. Press and release the **Power** button.
   4. After the device begins to boot, release the **Volume Up** button.
   5. Select **Boot configuration**.
   6. Do one of the following:
      * Select **PXE boot**, and drag it to the top of the list. Alternatively, you can swipe left on the network adapter to boot to the device immediately. This won’t affect the boot order.
      * Select the USB flash drive that holds the boot media.
3. Select **Exit**, and then select **Restart Now**.
4. When prompted, select **Enter** for network boot service.
5. Windows PE will load into memory, and the Task Sequence Wizard will start. Select **Next** to continue.
6. Select the task sequence that you imported earlier, and then select **Next**.
7. After the disk configuration is applied, you’ll be prompted to specify a computer name for the device. The user interface will display a recommended computer name based on the serial number of the Surface Pro device. You can either accept the proposed name or specify a new one. Follow the instructions on the computer name assignment screen. When you select **Accept**, the deployment begins.
8. The rest of the deployment process is automatic and doesn’t ask for any more user input.
9. After the deployment task sequence finishes configuring the device, you’ll see the following configuration screen that asks you to configure the Microsoft Teams Rooms application settings.
10. Plug the Surface Pro into the Microsoft Teams Rooms console, and configure the application settings.
11. Validate that the capabilities listed in [Microsoft Teams Rooms help](https://support.office.com/article/Skype-Room-Systems-version-2-help-e667f40e-5aab-40c1-bd68-611fe0002ba2) are working on the deployed device.

To troubleshoot a failed installation, check the **SMSTS.log** file, which logs all the steps executed in a Configuration Manager task sequence.

The SMSTS.log file is stored on one of a number of paths, depending on the stage of the build process. Check the following table to identify the path to the SMSTS.log file.

|  |  |
| --- | --- |
| **Deployment phase** | **Task sequence log path** |
| WinPE, before HDD format | X:\Windows\Temp\smstslog\smsts.log |
| WinPE, after HDD format | C:\\_SMSTaskSequence\Logs\Smstslog\smsts.log |
| Operating system deployed, before the Configuration Manager agent was installed | c:\\_SMSTaskSequence\Logs\Smstslog\smsts.log |
| Operating system and the Configuration Manager agent deployed | %windir%\System32\ccm\logs\Smstslog\smsts.log |
| Task sequence execution complete | %windir%\System32\ccm\logs\smsts.log |

**Tip**

You can select **F8** at any time during the task sequence to open a command console, and then get access to the SMSTS.log file.

To troubleshoot PXE boot issues, check the two log files on the Configuration Manager server that are specific to PXE actions:

* **Pxecontrol.log**, located in the Configuration Manager installation logs directory
* **Smspxe.log**, located in Configuration Manager Management Point (MP) logs directory

For a complete list of the log files that you can use to further troubleshoot your Configuration Manager installation, see [Log files in System Center Configuration Manager](https://docs.microsoft.com/sccm/core/plan-design/hierarchy/log-files).

**Deploy Microsoft Teams Rooms management with Azure Monitor**

This article discusses how to set up and deploy integrated, end-to-end management of Microsoft Teams Rooms devices by using Azure Monitor.

You can configure Log Analytics within Azure Monitor to provide basic telemetry and alerts that will help you manage Microsoft Teams Rooms meeting room devices. As your management solution matures, you might decide to deploy additional data and management capabilities to create a more detailed view of device availability and performance.

By following this guide, you can use a dashboard like the following example to get detailed status reporting for device availability, application and hardware health, and Microsoft Teams Rooms application and operating system version distribution.

At a high level, you need to perform the following tasks:

1. [Validate Log Analytics configuration](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#validate_LogAnalytics)
2. [Configure test devices for Log Analytics management setup](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#configure_test_devices)
3. [Map custom fields](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#Custom_fields)
4. [Define the Microsoft Teams Rooms views in Log Analytics](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#Define_Views)
5. [Define alerts](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#Alerts)
6. [Configure all devices for Monitoring](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#configure_all_devices)
7. [Configure additional Azure Monitor solutions](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy#Solutions)

**Important**

Although with minimal configuration, Azure Monitor Log Analytics can monitor a computer running a Windows operating system, there are still some Microsoft Teams Rooms–specific steps that you need to take before you start deploying agents to all Microsoft Teams Rooms devices. Therefore, we highly recommend you perform all configuration steps in the right order for a controlled setup and configuration. The quality of the end result very much depends on the quality of the initial configuration.

**Validate Log Analytics configuration**

You need to have a Log Analytics workspace to start collecting logs from Microsoft Teams Rooms devices. A workspace is a unique Log Analytics environment with its own data repository, data sources, and solutions. If you already have an existing Log Analytics workspace, you might use it to monitor your Microsoft Teams Rooms deployment or alternatively, you can create a dedicated Log Analytics workspace specific to your Microsoft Teams Rooms monitoring needs.

If you need to create a new Log Analytics workspace, follow the instructions in the article [Create a Log Analytics workspace in the Azure portal](https://docs.microsoft.com/azure/azure-monitor/learn/quick-create-workspace)

**Note**

To use Log Analytics with Azure Monitor, you need to have an active Azure subscription. If you don’t have an Azure subscription, you can create [**a free trial subscription**](https://azure.microsoft.com/free) as a starting point.

**Configure Log Analytics to collect Microsoft Teams Rooms event logs**

Log Analytics only collects events from the Windows event logs that are specified in the settings. For each log, only the events with the selected severities are collected.

You need to configure Log Analytics to collect the logs required to monitor Microsoft Teams Rooms device and application status. Microsoft Teams Rooms devices use the **Skype Room System** event log.

To configure Log Analytics to collect the Microsoft Teams Rooms events, see [Windows event log data sources in Azure Monitor](https://docs.microsoft.com/azure/azure-monitor/platform/data-sources-windows-events)

**Important**

Configure Windows Event Log settings and enter **Skype Room System** as event log name, and then select the **Error**, **Warning**, and **Information** check boxes.

**Configure test devices for Azure Monitoring**

You need to prepare Log Analytics to be able to monitor Microsoft Teams Rooms–related events. To start with, you need to deploy Microsoft Monitoring agents to just one or two Microsoft Teams Rooms devices that you have physical access to, and get those test devices generate some data and push it to the Log Analytics workspace.

**Install Microsoft Monitoring agents to test devices**

Deploy the Microsoft Monitoring agent to the test devices by using the instructions provided in [Connect Windows computers to the Log Analytics service in Azure](https://docs.microsoft.com/azure/azure-monitor/platform/agent-windows). This article provides detailed information about the steps for deploying Microsoft Monitoring Agent for Windows, instructions for obtaining the Log Analytics ***Workspace ID*** and the ***primary key*** to get Microsoft Teams Rooms devices connected to your Azure Monitor deployment, and steps to verify agent connectivity to Log Analytics instance.

**Generate sample Microsoft Teams Rooms events**

After the Microsoft Monitoring agent is deployed onto the test devices, verify that the required event log data is collected by Azure Monitor.

**Note**

Reboot the device after the installation of the Microsoft Monitoring agent, and make sure that Microsoft Teams Rooms Meeting app is started, so that it can generate new events into the Event Log.

1. Sign in to the [Microsoft Azure portal](https://portal.azure.com/) and go to Log Analytics and select your workspace.
2. List the heartbeat events generated by a Microsoft Teams Rooms device:
   1. Select your workspace and go to **Logs** and use a query to retrieve the heartbeat records that will have the custom fields for Microsoft Teams Rooms.
   2. Sample query: Event | where Source == "SRS-App" and EventID == 2000
3. Make sure that the query returns log records that include events generated by the Microsoft Teams Rooms meetings app.
4. Generate a hardware issue, and validate that the required events are logged in Azure Log Analytics.
   1. Unplug one of the peripheral devices on the test Microsoft Teams Rooms system. This could be the camera, speakerphone, microphone, or Front Room Display
   2. Wait 10 minutes for the event log to be populated in Azure Log Analytics.
   3. Use a query to list hardware error events: Event | where Source == "SRS-App" and EventID == 3001
5. Generate an application issue, and validate that the required events are logged.
   1. Modify Microsoft Teams Rooms application configuration, and type an incorrect Session Initiation Protocol (SIP) address/password pair.
   2. Wait 10 minutes for the event log to be populated in Azure Log Analytics.
   3. Use a query to list application error events: Event | where Source == "SRS-App" and EventID == 2001 and EventLevel == 1

**Important**

These sample event logs are required before custom fields can be configured. Don’t proceed to the next step until you have collected the required event logs.

**Map custom fields**

You use custom fields to extract specific data from the event logs. You need to define custom fields that will be used later with your tiles, dashboard views, and alerts. See [Custom fields in Log Analytics](https://docs.microsoft.com/azure/azure-monitor/platform/custom-fields) and become familiar with the concepts before you start creating your custom fields.

To extract your custom fields out of the captured event logs, follow these steps:

1. Sign in to the [Microsoft Azure portal](https://portal.azure.com/) and go to Log Analytics and select your workspace.
2. List the events generated by a Microsoft Teams Rooms device:
   1. Go to **Logs** and use a query to retrieve the records that will have the custom field.
   2. Sample query: Event | where Source == "SRS-App" and EventID == 2000
3. Select one of the records, select the button to the left, and start the field extraction wizard.
4. Highlight the data you’d like to extract from the RenderedDescription and provide a Field Title. The field names that you should use are provided in Table 1.
5. Use the mappings shown in *Table 1*. Log Analytics will automatically append the **\_CF** string when you define the new field.

**Important**

Remember that all JSON and Log Analytics fields are case-sensitive.

Pay attention to the queries required for each custom field in the table below. You need to use the correct queries for Log Analytics to successfully extract custom field values.

**Table 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **JSON field** | **Log Analytics custom field** | **Event ID** | **Query to use with the extraction** |
| Description | SRSEventDescription | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| ResourceState | SRSResourceState | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| OperationName | SRSOperationName | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| OperationResult | SRSOperationResult | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| OS | SRSOSVersion | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| OSVersion | SRSOSLongVersion | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| Alias | SRSAlias | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| DisplayName | SRSDisplayName | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| AppVersion | SRSAppVersion | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| IPv4Address | SRSIPv4Address | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| IPv6Address | SRSIPv6Address | **2000** | Event | where Source == "SRS-App" and EventID == 2000 |
| Conference Microphone status | SRSConfMicrophoneStatus | **3001** | Event | where Source == "SRS-App" and EventID == 3001 |
| Conference Speaker status | SRSConfSpeakerStatus | **3001** | Event | where Source == "SRS-App" and EventID == 3001 |
| Default Speaker status | SRSDefaultSpeakerStatus | **3001** | Event | where Source == "SRS-App" and EventID == 3001 |
| Camera status | SRSCameraStatus | **3001** | Event | where Source == "SRS-App" and EventID == 3001 |
| Front of Room Display status | SRSFORDStatus | **3001** | Event | where Source == "SRS-App" and EventID == 3001 |
| Motion Sensor status | SRSMotionSensorStatus | **3001** | Event | where Source == "SRS-App" and EventID == 3001 |
| HDMI Ingest status | SRSHDMIIngestStatus | **3001** | Event | where Source == "SRS-App" and EventID == 3001 |

**Define the Microsoft Teams Rooms views in Log Analytics**

After data is collected and custom fields are mapped, you can use View Designer to develop a dashboard containing various tiles to monitor Microsoft Teams Rooms events. Use View Designer to create the following tiles. For more information, see [Create custom views by using View Designer in Log Analytics](https://docs.microsoft.com/azure/azure-monitor/platform/view-designer)

**Note**

Previous steps in this guide should have been completed for the dashboard tiles to work properly.

**Create a Microsoft Teams Rooms dashboard by using the import method**

You can import an Microsoft Teams Rooms dashboard and start monitoring your devices quickly. Take the following steps to import the dashboard:

1. Get the [SkypeRoomSystems\_v2.omsview](https://go.microsoft.com/fwlink/?linkid=835675) dashboard file.
2. Sign in to the [Microsoft Azure portal](https://portal.azure.com/) and go to Log Analytics and select your workspace.
3. Open **View Designer**.
4. Select **Import**, and then select the **SkypeRoomSystems\_v2.omsview** file.
5. Select **Save**.

**Create a Microsoft Teams Rooms dashboard manually**

Alternatively, you can create your own dashboard and add only the tiles that you wish to monitor.

**Configure the Overview Tile**

1. Open **View Designer**.
2. Select **Overview Tile**, and then select **Two numbers** from the gallery.
3. Name the tile **Microsoft Teams Rooms**.
4. Define the **First Tile**:  
    **Legend:** Devices that sent a heartbeat at least once within the last month  
    **Query:** Event | where EventLog == "Skype Room System" and TimeGenerated > ago(30d) | summarize TotalSRSDevices = dcount(Computer)
5. Define the **Second Tile**:  
    **Legend:** Active devices that sent a heartbeat within the last hour  
    **Query:** Event | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" and TimeGenerated > ago(1h) | summarize TotalSRSDevices = dcount(Computer)
6. Select **Apply**.

**Create a tile that displays active devices**

1. Select **View Dashboard** to start adding your tiles.
2. Select **Number & list** from the gallery
3. Define the **General** properties:  
    **Group Title:** Heartbeat Status  
    **New Group:** Selected
4. Define the **Tile** properties:  
    **Legend:** Active devices (heartbeat sent in the last 20 minutes)  
    **Tile Query:** Event | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" and TimeGenerated > ago(20m) | summarize AggregatedValue = count() by Computer | count
5. Define the **List** properties:  
    **List Query:** Event | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" and TimeGenerated > ago(20m) | summarize TimeGenerated = max(TimeGenerated) by Computer | order by TimeGenerated
6. Define **Column Titles**:  
    **Name:** Computer Name  
    **Value:** Last Heartbeat
7. Define **Navigation Query**.  
    search {selected item} | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" | summarize arg\_max(TimeGenerated, \*) by Computer | project TimeGenerated, Computer, SRSAlias\_CF, SRSAppVersion\_CF, SRSOSVersion\_CF, SRSOSLongVersion\_CF, SRSIPv4Address\_CF, SRSIPv6Address\_CF, SRSOperationName\_CF, SRSOperationResult\_CF, SRSResourceState\_CF, SRSEventDescription\_CF
8. Select **Apply**, and then **Close**.

**Create a tile that displays devices that have connectivity issues**

1. Select **Number & list** from the gallery, and then add a new tile.
2. Define the **General** properties:  
    **Group Title:** Leave empty  
    **New Group:** Not Selected
3. Define the **Tile** properties:  
    **Legend:** Inactive Devices (no heartbeat message sent in the last 20 minutes)  
    **Tile Query:** Event | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" | summarize LastHB = max(TimeGenerated) by Computer | where LastHB < ago(20m) | count
4. Define the **List** properties:  
    **List Query:** Event | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" | summarize TimeGenerated = max(TimeGenerated) by Computer | where TimeGenerated < ago(20m) | order by TimeGenerated
5. Define **Column Titles**:  
    **Name:** Computer Name  
    **Value:** Last Heartbeat
6. Define **Navigation Query**:  
    search {selected item} | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" | summarize arg\_max(TimeGenerated, \*) by Computer | project TimeGenerated, Computer, SRSAlias\_CF, SRSAppVersion\_CF, SRSOSVersion\_CF, SRSOSLongVersion\_CF, SRSIPv4Address\_CF, SRSIPv6Address\_CF, SRSOperationName\_CF, SRSOperationResult\_CF, SRSResourceState\_CF, SRSEventDescription\_CF
7. Select **Apply**, and then **Close**.

**Create a tile that displays devices that have a hardware error**

1. Select **Number & list** from the gallery, and then add a new tile.
2. Define the **General** properties:  
    **Group Title:** Hardware Status  
    **New Group:** Selected
3. Define the **Tile** properties:  
    **Legend:** Devices that experienced a hardware error in the last hour  
    **Tile Query:** Event | where EventLog == "Skype Room System" and EventLevelName == "Error" and EventID == "3001" and TimeGenerated > ago(1h) | summarize AggregatedValue = count() by Computer | count
4. Define the **List** properties:  
    **List Query:** Event | where EventLog == "Skype Room System" and EventLevelName == "Error" and EventID == "3001" and TimeGenerated > ago(1h) | summarize TimeGenerated = max(TimeGenerated) by Computer | order by TimeGenerated
5. Define **Column Titles**:  
    **Name:** Computer Name  
    **Value:** Last Error
6. Define **Navigation Query**:  
    search {selected item} | where EventLog == "Skype Room System" and EventID == 3001 and EventLevelName == "Error" | summarize arg\_max(TimeGenerated, \*) by Computer | project TimeGenerated, Computer, SRSAlias\_CF, SRSAppVersion\_CF, SRSOSVersion\_CF, SRSOSLongVersion\_CF, SRSIPv4Address\_CF, SRSIPv6Address\_CF, SRSOperationName\_CF, SRSOperationResult\_CF, SRSResourceState\_CF, SRSConfMicrophoneStatus\_CF, SRSConfSpeakerStatus\_CF, SRSDefaultSpeakerStatus\_CF, SRSCameraStatus\_CF, SRSFORDStatus\_CF, SRSMotionSensorStatus\_CF, SRSHDMIIngestStatus\_CF, SRSEventDescription\_CF | sort by TimeGenerated desc
7. Select **Apply**, and then **Close**.

**Create a tile that displays Microsoft Teams Rooms Operating System versions**

1. Select **Donut & list** from the gallery, and then add a new tile.
2. Define the **General** properties:  
    **Group Title:** Operating System details  
    **New Group:** Selected
3. Define the **Header** properties:  
    **Title:** Operating System versions  
    **Subtitle:** Devices running specific OS versions
4. Define the **Donut** properties:  
    **Query:** Event | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" | summarize OS\_Version = max(SRSOSLongVersion\_CF) by Computer | summarize AggregatedValue = count() by OS\_Version | sort by OS\_Version asc  
    **Center Text:** Devices  
    **Operation:** Sum
5. Define the **List** properties.  
    **List Query:** Event | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" | summarize SRSOSLongVersion\_CF = max(SRSOSLongVersion\_CF) by Computer | sort by Computer asc  
    **Hide Graph:** Selected  
    **Enable Sparklines:** Not selected
6. Define **Column Titles**.  
    **Name:** Computer Name  
    **Value:** Leave Empty
7. Define **Navigation Query**.  
    search {selected item} | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" | summarize arg\_max(TimeGenerated, \*) by Computer | project TimeGenerated, Computer, SRSDisplayName\_CF, SRSAlias\_CF, SRSAppVersion\_CF, SRSOSVersion\_CF, SRSOSLongVersion\_CF, SRSIPv4Address\_CF, SRSIPv6Address\_CF, SRSOperationName\_CF, SRSOperationResult\_CF, SRSResourceState\_CF, SRSEventDescription\_CF
8. Select **Apply** and then **Close**.

**Create a tile that displays Microsoft Teams Rooms application versions**

1. Select **Donut & list** from the gallery, and then add a new tile.
2. Define the **General** properties:  
    **Group Title:** Microsoft Teams Rooms application details  
    **New Group:** Selected
3. Define the **Header** properties:  
    **Title:** Application versions  
    **Subtitle:** Devices running specific application versions
4. Define the **Donut** properties:  
    **Query:** Event | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" | summarize App\_Version = max(SRSAppVersion\_CF) by Computer | summarize AggregatedValue = count() by App\_Version | sort by App\_Version asc  
    **Center Text:** Devices  
    **Operation:** Sum
5. Define the **List** properties.  
    **List Query:** Event | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" | summarize SRSAppVersion\_CF = max(SRSAppVersion\_CF) by Computer | sort by Computer asc  
    **Hide Graph:** Selected  
    **Enable Sparklines:** Not selected
6. Define **Column Titles**.  
    **Name:** Computer Name  
    **Value:** Leave Empty
7. Define **Navigation Query**.  
    search {selected item} | where EventLog == "Skype Room System" and SRSOperationName\_CF == "Heartbeat" | summarize arg\_max(TimeGenerated, \*) by Computer | project TimeGenerated, Computer, SRSAlias\_CF, SRSAppVersion\_CF, SRSOSVersion\_CF, SRSOSLongVersion\_CF, SRSIPv4Address\_CF, SRSIPv6Address\_CF, SRSOperationName\_CF, SRSOperationResult\_CF, SRSResourceState\_CF, SRSEventDescription\_CF
8. Select **Apply** and then **Close**.

**Create a tile that displays devices that have an application error**

1. Select **Number & list** from the gallery, and then add a new tile.
2. Define the **General** properties.  
    **Group Title:** Leave empty  
    **New Group:** Not Selected
3. Define the **Tile** properties.  
    **Legend:** Devices that experienced an application error in the last hour  
    **Tile Query:** Event | where EventLog == "Skype Room System" and EventLevelName == "Error" and EventID == "2001" and TimeGenerated > ago(1h) | summarize AggregatedValue = count() by Computer | count
4. Define the **List** properties.  
    **List Query:** Event | where EventLog == "Skype Room System" and EventLevelName == "Error" and EventID == "2001" and TimeGenerated > ago(1h) | summarize TimeGenerated = max(TimeGenerated) by Computer | order by TimeGenerated
5. Define **Column Titles**.  
    **Name:** Computer Name  
    **Value:** Last Error
6. Define **Navigation Query**.  
    search {selected item} | where EventLog == "Skype Room System" and EventID == 2001 and EventLevelName == "Error" | summarize arg\_max(TimeGenerated, \*) by Computer | project TimeGenerated, Computer, SRSAlias\_CF, SRSAppVersion\_CF, SRSOSVersion\_CF, SRSOSLongVersion\_CF, SRSIPv4Address\_CF, SRSIPv6Address\_CF, SRSOperationName\_CF, SRSOperationResult\_CF, SRSResourceState\_CF, SRSEventDescription\_CF | sort by TimeGenerated desc
7. Select **Apply** and then **Close**.

**Create a tile that displays devices that have been restarted**

1. Select **Number & list** from the gallery, and then add a new tile.
2. Define the **General** properties.  
    **Group Title:** Leave empty  
    **New Group:** Not Selected
3. Define the **Tile** properties.  
    **Legend:** Devices where the application was restarted in the last 24 hours, and number of restarts  
    **Tile Query:** Event | where EventLog == "Skype Room System" and EventID == "4000" and TimeGenerated > ago(24h) | summarize AggregatedValue = count() by Computer | count
4. Define the **List** properties.  
    **List Query:** Event | where EventLog == "Skype Room System" and EventID == "4000" and TimeGenerated > ago(24h) | order by TimeGenerated | summarize AggregatedValue = count(EventID) by Computer
5. Define **Column Titles**.  
    **Name:** Computer Name  
    **Value:** Number of Restarts
6. Define **Navigation Query**.  
    search {selected item} | where EventLog == "Skype Room System" and EventID == "4000" and TimeGenerated > ago(24h) | project TimeGenerated, Computer, SRSAlias\_CF, SRSAppVersion\_CF, SRSOSVersion\_CF, SRSOSLongVersion\_CF, SRSIPv4Address\_CF, SRSIPv6Address\_CF, SRSOperationName\_CF, SRSOperationResult\_CF, SRSResourceState\_CF, SRSEventDescription\_CF
7. Select **Apply** and then **Close**.
8. Select **Save** to save your dashboard.

Now you’ve completed creating your views.

**Configure Alerts in Azure Monitor**

Azure Monitor can raise alerts to notify the administrators, when a Microsoft Teams Rooms console encounters an issue.

Azure Monitor includes a built-in alerting mechanism that runs through scheduled log searches at regular intervals. If the results of the log search match some particular criteria, an alert record is created.

The rule can then automatically run one or more actions to proactively notify you of the alert or invoke another process. The possible options with alerts are:

* Sending an email
* Invoking an external process through an HTTP POST request
* Starting a runbook in Azure Automation service

See [Log alerts in Azure Monitor](https://docs.microsoft.com/azure/azure-monitor/platform/alerts-unified-log) to learn more about the alerts in Azure Monitor.

**Note**

The following examples send email alerts when a Microsoft Teams Rooms device generates a hardware or an application error.

**Configure an email alert for Microsoft Teams Rooms hardware issues**

Configure an alert rule that checks for Microsoft Teams Rooms devices that have encountered hardware issues within the last hour.

1. Sign in to the [Microsoft Azure portal](https://portal.azure.com/) and go to Log Analytics and select your workspace.
2. Navigate to your Log Analytics workspace and select **Alerts** and then select **New alert rule**
3. Select **Add condition** and then **Custom log search**
4. Enter the following query to the Search query text box.  
     
     
     
    Copy  
    Event
5. | where EventLog == "Skype Room System" and EventLevelName == "Error" and EventID == "3001" and TimeGenerated > ago(1h)
6. | summarize arg\_max(TimeGenerated, \*) by Computer
7. | project TimeGenerated, Computer, SRSAlias\_CF, SRSAppVersion\_CF, SRSOSVersion\_CF, SRSOSLongVersion\_CF, SRSIPv4Address\_CF, SRSIPv6Address\_CF, SRSOperationName\_CF, SRSOperationResult\_CF, SRSResourceState\_CF, SRSConfMicrophoneStatus\_CF, SRSConfSpeakerStatus\_CF, SRSDefaultSpeakerStatus\_CF, SRSCameraStatus\_CF, SRSFORDStatus\_CF, SRSMotionSensorStatus\_CF, SRSHDMIIngestStatus\_CF, SRSEventDescription\_CF
8. |sort by TimeGenerated desc
10. Configure the Alert logic settings:  
     **Based on:** Number of results  
     **Condition:** Greater then  
     **Treshold:** 0
11. Configure Evaluation settings and select **Done**:   
     **Period (in minutes):** 60  
     **Frequency (in minutes):** 60
12. Configure action groups:
    1. Select **Create New**
    2. Provide suitable names for the *Action group name* and *Short Name* fields.
    3. Specify a unique *Action Name* and select **Email/SMS/Push/Voice**, and then select **Edit details**.
    4. Select the Email checkbox and provide the email address of the person or group that will recieve the alerts.
    5. You may also provide your phone number to get notified with SMS, a voice call or both.
    6. Select **OK**.
13. **Customize Actions** if you like to override the subject line of the alert emails.
14. Specify a rule name and description.  
     **Rule Name:** Microsoft Teams Rooms Hardware Failure Alert  
     **Description:** List of devices that encountered a hardware issue within the last hour
15. Select the intended severity and make sure the rule is enabled.
16. Select **Create alert rule**.

**Configure an email alert for Microsoft Teams Rooms application issues**

Repeat the same procedure but use the following query to list devices that have encountered application issues within the last hour.

Copy

```

Event

| where EventLog == "Skype Room System" and EventLevelName == "Error" and EventID == "2001" and TimeGenerated > ago(1h)

| summarize arg\_max(TimeGenerated, \*) by Computer

| project TimeGenerated, Computer, SRSAlias\_CF, SRSAppVersion\_CF, SRSOSVersion\_CF, SRSOSLongVersion\_CF, SRSIPv4Address\_CF, SRSIPv6Address\_CF, SRSOperationName\_CF, SRSOperationResult\_CF, SRSResourceState\_CF, SRSEventDescription\_CF

| sort by TimeGenerated desc

```

Now you’ve completed defining alerts. You can define additional alerts by using the examples above.

When an alert is generated, you’ll get an email that lists the devices that encountered an issue within the last hour.

**Configure all devices for Azure Monitoring**

After the dashboards and alerts are configured, you can set up and configure Microsoft Monitoring agent on all Microsoft Teams Rooms devices to complete your monitoring deployment.

Although you can install and configure the Microsoft Monitoring agent manually on each device, we highly recommend you leverage existing software deployment tools and methods.

If you’re building your Microsoft Teams Rooms devices for the first time, you might want to include the Microsoft Monitoring agent setup and configuration steps as part of your build process. For more information, see [Install the agent using the command line](https://docs.microsoft.com/azure/azure-monitor/platform/agent-windows#install-the-agent-using-the-command-line).

**Deploying Microsoft Monitoring agent by using a Group Policy Object (GPO)**

If you already deployed your Microsoft Teams Rooms devices before you implement Azure Monitoring, you can use the provided script to set up and configure the agents by using Active Directory group policy objects.

1. Create a shared network path and grant read access to **Domain Computers** group.
2. Download the 64-bit version of the Microsoft Monitoring Agent for Windows from <https://go.microsoft.com/fwlink/?LinkID=517476>
3. Extract the contents of the setup package into the network share.
   1. Open a Command Prompt window, and then execute **MMASetup-AMD64.exe /c**
   2. Specify the share you just created, and extract the content.
4. Create a new Group Policy Object and assign it to the organizational unit where Microsoft Teams Rooms machine accounts are located.
5. Configure PowerShell execution policy:
   1. Edit the newly created Group Policy Object and navigate to Computer Configuration \ Policies \ Administrative Templates \ Windows Components \ Windows PowerShell
   2. Enable the **Turn on Script Execution** and set **Execution Policy** to **Allow Local Scripts**.
6. Configure the startup script:
   1. Copy the following script and save it as Install-MMAgent.ps1.
   2. Modify WorkspaceId, WorkspaceKey, and SetupPath parameters to match your configuration.
   3. Edit the same Group Policy Object and navigate to Computer Configuration \ Policies \ Windows Settings \ Scripts (Startup/Shutdown)
   4. Double-click to select **Startup**, and then select **PowerShell Scripts**.
   5. Select **Show Files**, and then copy the **Install-MMAgent.ps1** file to that folder.
   6. Select **Add**, and then **Browse**.
   7. Select the ps1 script you just copied.
7. Microsoft Teams Rooms devices should install and configure the Microsoft Monitoring agent with the second reboot.

Copy

# Install-MMAgent.ps1

<#

Date: 04/20/2018

Script: Install-MMAgent.ps1

Version: 1.0

#>

# Set the parameters

$WorkspaceId = "<your workspace id>"

$WorkspaceKey = "<your workspace key>"

$SetupPath = "\\Server\Share"

$SetupParameters = "/qn NOAPM=1 ADD\_OPINSIGHTS\_WORKSPACE=1 OPINSIGHTS\_WORKSPACE\_AZURE\_CLOUD\_TYPE=0 OPINSIGHTS\_WORKSPACE\_ID=$WorkspaceId OPINSIGHTS\_WORKSPACE\_KEY=$WorkspaceKey AcceptEndUserLicenseAgreement=1"

# $SetupParameters = $SetupParameters + " OPINSIGHTS\_PROXY\_URL=<Proxy server URL> OPINSIGHTS\_PROXY\_USERNAME=<Proxy server username> OPINSIGHTS\_PROXY\_PASSWORD=<Proxy server password>"

# Start PowerShell logging

Start-Transcript -Path C:\Temp\MMA-Install.Log

# Check if the Microsoft Monitoring Agent is installed

$mma = New-Object -ComObject 'AgentConfigManager.MgmtSvcCfg'

# Check if the Microsoft Monitoring agent is installed

if (!$mma)

{

#Install agent

Start-Process -FilePath "$SetupPath\Setup.exe" -ArgumentList $SetupParameters -ErrorAction Stop -Wait

}

# Check if the agent has a valid configuration

$CheckMMA = $mma.GetCloudWorkspace($WorkspaceId).AgentId

if (!$CheckMMA)

{

# Apply new configuration

$mma.AddCloudWorkspace($WorkspaceId, $WorkspaceKey)

$mma.ReloadConfiguration()

}

Stop-Transcript

**Note**

You can refer to the article [**Managing and maintaining the Log Analytics agent**](https://docs.microsoft.com/azure/azure-monitor/platform/agent-manage) when you need to reconfigure an agent, move it to a different workspace, or modify proxy settings after the initial installation.

**Additional Solutions**

Azure Monitor provides built-in management solutions through its [solution gallery](https://docs.microsoft.com/azure/azure-monitor/insights/solutions) to further help you monitor your environment. We highly recommend that you add [Alert Management](https://docs.microsoft.com/azure/azure-monitor/platform/alert-management-solution) and [Azure Log Analytics Agent Health](https://docs.microsoft.com/azure/azure-monitor/insights/solution-agenthealth) solutions to your workspace as well.

**Note**

The Agent Health solution can help you identify outdated or broken Microsoft Monitoring agents within your environment, and the Alert Management solution provides details about the alerts that have been raised within a given period.

**Migrate Lync Room System (LRS) devices to Microsoft Teams Rooms**

Lync Room System (LRS) devices with Skype Room System Version 1 (SRS v1) software has reached [end of support on October 9, 2018](https://support.microsoft.com/en-us/help/4043450/products-reaching-end-of-support-for-2018). This means Skype Room Systems v1 software will no longer get any product updates or fixes anymore. Customers with Lync Room System devices using Skype Room System v1 software are advised to upgrade their devices to Microsoft Teams Rooms.

Microsoft Teams Rooms software works with Microsoft Teams in addition to Skype for Business Server and Online services for meetings and calling on all Microsoft Teams Rooms supported devices.

Your existing devices **may** continue to work after the end of Skype Room System v1 software support. However, if this software hits a software bug that needs Microsoft to release a fix, it will not be supported. SRS v1 uses TLS 1.0/ 1.1 which will be deprecated by Microsoft in the future. You can learn more about [Preparing for TLS 1.0/1.1 Deprecation](https://techcommunity.microsoft.com/t5/Skype-for-Business-Blog/Preparing-for-TLS-1-0-1-1-Deprecation-O365-Skype-for-Business/bc-p/223608). Microsoft Teams Rooms is adding support for TLS 1.2 and will continue to work past October 31, 2018. Skype for Business on-premises customers should not disable TLS 1.0/1.1 until Microsoft Teams Rooms announces support for TLS 1.2 regardless of general guidelines on TLS 1.0/1.1 deprecation.

**Which devices are affected?**

Here is the list of the devices that are affected by this change:

* Crestron RL
* [Crestron RL2](https://www.crestron.com/en-US/Products/Featured-Solutions/Crestron-RL-2)
* [SMART Room systems](https://support.smarttech.com/en/hardware/room-systems-skype)
* [Polycom CX8000](http://www.polycom.com/products-services/products-for-microsoft/skype-for-business/cx8000.html)

**Upgrade options**

There are multiple options for upgrading Lync Room Systems to the next generation of Microsoft Teams Rooms.

**Crestron hardware Trade-in program**

Crestron will provide an upgrade to the [Crestron SR system](https://www.crestron.com/en-us/products/featured-solutions/crestron-sr) or equivalent for all Non-Crestron Lync Room System customers (e.g Smart or Polycom LRS). See details of this program [here](https://support.crestron.com/app/answers/answer_view/a_id/1000220) or email Crestron LRS support.

**Crestron RL2 upgrade to Microsoft Teams Rooms**

Existing Crestron RL2 (also referred to as Crestron RL200) customers can acquire an upgrade kit to upgrade current RL2 to RL3 using a for a minimal cost per device. See details of this program [here](https://crestron.com/en-US/Products/Workspace-Solutions/Unified-Communications/Crestron-RL-2/CCS-UC-250-KIT).

**SMART Room Systems upgrade**

For SMART LRS customers, apart from Crestron hardware trade-in program, SMART is also working on providing a solution to upgrade to Microsoft Teams Rooms. This upgrade will be provided by SMART Technologies Inc. to customer under product support. Please see more about this [here](https://support.smarttech.com/docs/hardware/room-systems-skype/srs-skype-v2/en/about/default.cshtml).

**What should you do?**

We recommend you plan to update Lync Room System devices to Microsoft Teams Rooms before TLS 1.0/1.1 deprecation using upgrade options mentioned above. Additionally, you may also consider replacing existing devices with new devices certified for Microsoft Teams Rooms. See [Room devices](https://aka.ms/roomdevices) for details and also take a look at [Microsoft Teams Rooms requirements](https://docs.microsoft.com/skypeforbusiness/plan-your-deployment/clients-and-devices/requirements).

**Note**

Touch and whiteboard functionality is not yet supported in Microsoft Teams Rooms. Touch and whiteboard support is currently planned for Microsoft Teams Rooms and will be added in 2019.

**Note**

Microsoft Teams Rooms software supports the TLS 1.2 protocol as of December 14, 2018 with app version 4.0.64.0. For on-premises customers, enabling communication over TLS 1.2 for Microsoft Teams Rooms requires Skype for Business Server 2015 Cumulative Update 9 (CU9) or Skype for Business Server 2019 Cumulative Update 1 (CU1). The change should not affect Skype for Business Online customers as client changes are forward and backward compliant.

**Microsoft Teams Rooms licenses**

The following table lists the licensing-dependant features that are available in Microsoft Teams Rooms and what licenses you need to buy to get them.

**Note**

The room that is being set up needs to be a user object and have these licenses assigned to it. The new Meeting Room license is now available in Office 365.

|  |  |  |  |
| --- | --- | --- | --- |
| **Microsoft Teams Rooms scenario** | **You currently have Office 365 Premium, Office 365 ProPlus, or Skype for Business Standalone Plan 2.**  **Here's what you need to buy:** | **You currently have an Enterprise-based plan.**  **Here's what you need to buy:** | **You have Skype for Business Server 2015 (on-premises or hybrid).**  **Here's what you need to buy:** |
| Join a scheduled meeting. | Skype for Business Standalone Plan 1 | E1, 3, 4, or 5 | Skype for Business Server Standard CAL |
| Initiate an ad-hoc meeting. | Skype for Business Standalone Plan 2 | E1, 3, 4, or 5 | Skype for Business Server Standard CAL  Skype for Business Server Enterprise CAL |
| Initiate an ad-hoc meeting and dial out from a meeting to phone numbers. | Skype for Business Standalone Plan 2 with Audio Conferencing  **Note:** Communications Credits are optional. | E1 or E3 with Audio Conferencing  OR  E5 | Skype for Business Standard CAL  Skype for Business Server Enterprise CAL |
| Give the room a phone number and make or receive a calls from the room or join an audio conference using a phone number. | Skype for Business Standalone Plan 2 with Office 365 Phone System and a Calling Plan  **Note:** Communications Credits are optional. | E1 or E3 with Office 365 Phone System and a Office 365 Calling Plan  OR  E5 | Skype for Business Server Standard CAL  Skype for Business Server Plus CAL |

**Use the right version of Windows 10**: For customers who want to deploy Windows 10 images to their devices, see [Configure a Microsoft Teams Rooms console](https://docs.microsoft.com/en-us/Skypeforbusiness/deploy/deploy-clients/console.md).

**Microsoft Teams Rooms maintenance and operations**

Read this topic to learn about management of Microsoft Teams Rooms, the next generation of Skype Room Systems.

Microsoft Teams Rooms is Microsoft's latest conferencing solution designed to transform your meeting room into a rich, collaborative experience. Users will enjoy its familiar Microsoft Teams or Skype for Business interface and IT administrators will appreciate an easily deployed and managed Windows 10 Skype Meeting app. Microsoft Teams Rooms is designed to leverage existing equipment like LCD panels for ease of installation to bring Microsoft Teams or Skype for Business into your meeting room.

With additional configuration, remote management is possible using Microsoft Azure Monitor as described in [Plan Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-plan), [Deploy Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy), [Manage Microsoft Teams Rooms devices with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy). You may also [Manage Microsoft Teams Rooms console settings remotely with an XML configuration file](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/xml-config-file), which includes applying a Custom display theme.

**Collecting logs on Microsoft Teams Rooms**

To collect logs, you must invoke the log collection script that ships with the Microsoft Teams Rooms app. In Admin mode, start an elevated command prompt, and issue the following command:

Copy

powershell -ExecutionPolicy unrestricted c:\rigel\x64\scripts\provisioning\ScriptLaunch.ps1 CollectSrsV2Logs.ps1

The logs will be output as a ZIP file in c:\rigel.

**Front of Room Display Settings**

Configure the Front of Room display to Extended mode. Doing so will ensure that the console UI is not duplicated on that display when you cycle power on the display.

**Note**

A consumer TV used as a front of room display needs to support/enable the Consumer Electronics Control (CEC) feature of HDMI so that it can switch automatically to an active video source from standby mode. This feature is not supported on all TVs.

**Microsoft Teams Rooms Reset (Factory Restore)**

If Microsoft Teams Rooms isn't running well, performing a factory reset might help. This can be done in the Settings app on the **Recovery** tab. Beneath **Reset this PC**, select **Get started**, and then **Remove everything**. Follow the remaining prompts to reset the device.

**Note**

There is a known issue where the Microsoft Teams Rooms can become unusable if the **Keep my files - Removes Apps and settings, but keeps your personal files** option is selected during the Windows Reset process. Do *not* use this option.

**Supported Remote Options**

The following table summarizes the possible remote operations and the methods you can use to accomplish them.

|  |  |  |
| --- | --- | --- |
| **Workgroup** | **Not domain joined** | **Domain joined** |
| Restart | Remote desktop  Remote Powershell | Remote desktop (requires further configuration)  Remote Powershell (requires further configuration)  SCCM |
| Update OS | Windows Update | Windows Update  WSUS |
| App update | Windows Store | Windows Store  SCCM |
| Skype Account Config | Not currently supported | Not currently supported |
| Access logs | Not currently supported | Not currently supported |

**Configuring Group Policy for Microsoft Teams Rooms**

This section covers system settings that Microsoft Teams Rooms depends on to function properly. When joining Microsoft Teams Rooms to a domain, ensure that your group policy doesn't override the settings in the following table.

|  |  |
| --- | --- |
| **Setting** | **Allows** |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon AutoAdminLogon = (REG\_SZ) 1 | Enables Microsoft Teams Rooms to boot up |
| Power Management -> On AC, turn screen off after 10 minutes  Power Management -> On AC, never put system to sleep | Enables Microsoft Teams Rooms to turn off attached displays and wake up automatically |
| net accounts /maxpwage:unlimited  Or equivalent means of disabling password expiration on the local account. Failure to do this will eventually cause the Skype account to fail logon complaining about an expired password. Note that this impacts all local accounts on the machine, and thus failure to set this will also cause the administrative account on the box to eventually expire as well. | Enables Skype account to always log in |

Transferring files using Group Policies is discussed in [Configure a File Item](https://technet.microsoft.com/library/cc772536%28v=ws.11%29.aspx).

**Note**

When Microsoft Teams Rooms device is compatible with the next version of Windows 10 OS, the device automatically updates to the next version through Windows Update. Microsoft Teams Rooms device should not be upgraded to next release of Windows 10 manually or via enabling Windows Update for Business (WUFB) group policies “Select the Windows readiness level for the updates you want to receive” and "Select when Preview Builds and Feature Updates are received" through GPO. A device with these group policies enabled is known to run into issues with Windows 10 OS update by Microsoft Teams Rooms app.

**Remote Management using PowerShell**

You can perform the following management operations remotely by using PowerShell (see the table below for script samples):

* Get attached devices
* Get app status
* Get system info
* Reboot system
* Retrieve logs
* Transfer files (requires a domain-joined Microsoft Teams Rooms)

**Note**

This functionality is off by default. You need to enable remote PowerShell for your environment on the Microsoft Teams Rooms system to perform the operations below. Refer to the documentation on [**Enable-PSRemoting**](https://technet.microsoft.com/library/hh849694.aspx) for information about how to enable remote PowerShell.

For example, you can enable Remote PowerShell as follows:

1. Sign in as Admin on a Microsoft Teams Rooms device.
2. Open an elevated PowerShell command prompt.
3. Enter the following command: Enable-PSRemoting -force

To perform a management operation:

1. Sign in to a PC with account credentials that have permission to run PowerShell commands on a Microsoft Teams Rooms device.
2. Open a regular PowerShell command prompt on the PC.
3. Copy the command text from the table below and paste it at the prompt.
4. Replace <Device fqdn> fields with FQDN values appropriate to your environment.
5. Replace *<path>* with the file name and local path of the master SkypeSettings.xml configuration file (or Theme image).

To Get Attached Devices

Copy

invoke-command {Write-Host "VIDEO DEVICES:"

gwmi -Class Win32\_PnPEntity | where {$\_.PNPClass -eq "Image"} | Format-Table Name,Status,Present; Write-Host "AUDIO DEVICES:"

gwmi -Class Win32\_PnPEntity | where {$\_.PNPClass -eq "Media"} | Format-Table Name,Status,Present; Write-Host "DISPLAY DEVICES:"

gwmi -Class Win32\_PnPEntity | where {$\_.PNPClass -eq "Monitor"} | Format-Table Name,Status,Present} -ComputerName <Device fqdn>

Get App Status

Copy

invoke-command { $package = get-appxpackage -User Skype -Name Microsoft.SkypeRoomSystem; if ($package -eq $null) {Write-host "SkypeRoomSystems not installed."} else {write-host "SkypeRoomSystem Version : " $package.Version}; $process = Get-Process -Name "Microsoft.SkypeRoomSystem" -ErrorAction SilentlyContinue; if ($process -eq $null) {write-host "App not running."} else {$process | format-list StartTime,Responding}} -ComputerName <Device fqdn>

Get System Info

Copy

invoke-command {gwmi -Class Win32\_ComputerSystem | Format-List PartOfDomain,Domain,Workgroup,Manufacturer,Model

gwmi -Class Win32\_Bios | Format-List SerialNumber,SMBIOSBIOSVersion} -ComputerName <Device fqdn>

Reboot System

Copy

invoke-command { Shutdown /r /t 0 } -ComputerName <Device fqdn>

Retrieve Logs

Copy

$targetDevice = "<Device fqdn> "

$logFile = invoke-command {$output = Powershell.exe -ExecutionPolicy Bypass -File C:\Rigel\x64\Scripts\Provisioning\ScriptLaunch.ps1 CollectSrsV2Logs.ps1

Get-ChildItem -Path C:\Rigel\\*.zip | Sort-Object -Descending -Property LastWriteTime | Select-Object -First 1} -ComputerName $targetDevice

$session = new-pssession -ComputerName $targetDevice

Copy-Item -Path $logFile.FullName -Destination .\ -FromSession $session; invoke-command {remove-item -force C:\Rigel\\*.zip} -ComputerName $targetDevice

Push an XML configuration file (or theme graphic)

Copy

$movefile = "<path>";

$targetDevice = "\\<Device fqdn> \Users\Skype\AppData\Local\Packages\Microsoft.SkypeRoomSystem\_8wekyb3d8bbwe\LocalState\SkypeSettings.xml";

Copy-Item $movefile $targetDevice

**Software updates**

By default, Microsoft Teams Rooms attempts to connect to the Windows Store to get the latest version of Microsoft Teams Rooms software, so the device will require regular internet access. Before contacting Microsoft with support issues, be sure the Microsoft Teams Rooms device is loaded with the latest version of the app.

By default, Microsoft Teams Rooms connects to Windows Update to retrieve operating system and USB peripheral device firmware updates, and installs them outside of configured business hours. You can configure business hours by signing into the administrator account and running the Settings app.

If you want to manage updates manually, and are unable to follow the normal procedure for [Microsoft Store for Business](https://businessstore.microsoft.com/store) to [Distribute offline apps](https://docs.microsoft.com/microsoft-store/distribute-offline-apps), you can acquire the appropriate APPX file and dependencies from the [deployment kit](https://go.microsoft.com/fwlink/?linkid=851168) (from the instructions to [Configure a Microsoft Teams Rooms console](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console)) that can be used with SCCM. The deployment kit release lags behind the store release, so it might not always match the latest available build.

**To update using Powershell**

1. Extract the package from the installation [MSI](https://go.microsoft.com/fwlink/?linkid=851168) to a share the device can access.
2. Run the following script targeting the Microsoft Teams Rooms devices, changing <share> to the device share as appropriate:

Copy

Add-AppxPackage -Update -ForceApplicationShutdown -Path '\\<share>\$oem$\$1\Rigel\x64\Ship\AppPackages\\*\\*.appx' -DependencyPath (Get-ChildItem '\\<share>\$oem$\$1\Rigel\x64\Ship\AppPackages\\*\Dependencies\x64\\*.appx' | Foreach-Object {$\_.FullName})

**Admin mode and device management**

Some management functions, like manually installing a private CA certificate, require placing the Surface Pro device in Admin mode.

**Switching to Admin Mode and back when the Microsoft Teams Rooms app is running**

1. Hang up any ongoing calls, and return to the home screen.
2. Select the Gear icon and bring up the menu (options are **Settings**, **Accessibility**, and **Restart Device** ).
3. Select **Settings**.
4. Enter the Administrator Password. The Setup screen will appear.  
     **Note** If the device isn't domain-joined, the local administrative account (username "Admin") will be used by default. The default password for this account is 'sfb' but it is recommended that your organization change this for security reasons as soon as possible. If the machine is domain-joined, you can sign in with an appropriately privileged domain account.
5. Select **Windows Settings** in the left column.
6. Choose **Go to Admin Sign-in**.
7. Enter the Administrator Password. This will gracefully log off the app and take you to the Windows login screen.
8. Log in to the desktop with your administrative credentials. You'll have the necessary privileges to manage the device.
9. Perform the necessary administrative tasks.
10. Sign out from the Admin account.
11. Return to Microsoft Teams Rooms by selecting the user account icon on the far left side of the screen and then selecting **Skype**.  
     If the **Skype** user is not listed, you might have to select **other user** and enter **.\skype** as the user name, and sign in.

The console is now back in its normal operation mode.The following procedure requires you to attach a keyboard to the device if one is not already attached.

**Switching to Admin Mode and back when the Microsoft Teams Rooms app crashes**

1. Press the Windows key five times in rapid succession. This will bring you to the Windows logon screen.
2. Log in to the desktop with your administrative credentials.  
     **Note** This method doesn't log the Skype user off or gracefully terminate the app, but you'd use it if the app wasn't responding and the other method wasn't available.
3. Perform the necessary administrative tasks.
4. Restart the machine when you're finished.  
    The console restarts into its normal operation mode, running the Microsoft Teams Rooms app. You can remove the keyboard, if it was attached to allow you to perform this procedure.  
    **Troubleshooting tips**

* Meeting invitations might not appear when sent across domain boundaries (for example, between two companies). In such cases, IT admins should decide whether to allow external users to schedule a meeting.
* Microsoft Teams Rooms doesn't support Exchange AutoDiscover redirects via Exchange 2010.
* In general, it's a good practice for IT admins to disable any audio endpoints they don't intend to use.
* In the event that a mirror image is displayed in room preview, the IT admin can correct by cycling camera power or flipping the image orientation using the camera remote control.
* Loss of console touchscreen access has been known to occur. In such cases, the issue is sometimes resolved by restarting the Microsoft Teams Rooms system.
* Loss of local audio when connecting a PC to console via wired ingest has been known to occur. In such cases, restarting the PC can resolve the local audio playback issue.

**Microsoft Teams Rooms maintenance and operations**

Read this topic to learn about management of Microsoft Teams Rooms, the next generation of Skype Room Systems.

Microsoft Teams Rooms is Microsoft's latest conferencing solution designed to transform your meeting room into a rich, collaborative experience. Users will enjoy its familiar Microsoft Teams or Skype for Business interface and IT administrators will appreciate an easily deployed and managed Windows 10 Skype Meeting app. Microsoft Teams Rooms is designed to leverage existing equipment like LCD panels for ease of installation to bring Microsoft Teams or Skype for Business into your meeting room.

With additional configuration, remote management is possible using Microsoft Azure Monitor as described in [Plan Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-plan), [Deploy Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy), [Manage Microsoft Teams Rooms devices with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy). You may also [Manage Microsoft Teams Rooms console settings remotely with an XML configuration file](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/xml-config-file), which includes applying a Custom display theme.

**Collecting logs on Microsoft Teams Rooms**

To collect logs, you must invoke the log collection script that ships with the Microsoft Teams Rooms app. In Admin mode, start an elevated command prompt, and issue the following command:

Copy

powershell -ExecutionPolicy unrestricted c:\rigel\x64\scripts\provisioning\ScriptLaunch.ps1 CollectSrsV2Logs.ps1

The logs will be output as a ZIP file in c:\rigel.

**Front of Room Display Settings**

Configure the Front of Room display to Extended mode. Doing so will ensure that the console UI is not duplicated on that display when you cycle power on the display.

**Note**

A consumer TV used as a front of room display needs to support/enable the Consumer Electronics Control (CEC) feature of HDMI so that it can switch automatically to an active video source from standby mode. This feature is not supported on all TVs.

**Microsoft Teams Rooms Reset (Factory Restore)**

If Microsoft Teams Rooms isn't running well, performing a factory reset might help. This can be done in the Settings app on the **Recovery** tab. Beneath **Reset this PC**, select **Get started**, and then **Remove everything**. Follow the remaining prompts to reset the device.

**Note**

There is a known issue where the Microsoft Teams Rooms can become unusable if the **Keep my files - Removes Apps and settings, but keeps your personal files** option is selected during the Windows Reset process. Do *not* use this option.

**Supported Remote Options**

The following table summarizes the possible remote operations and the methods you can use to accomplish them.

|  |  |  |
| --- | --- | --- |
| **Workgroup** | **Not domain joined** | **Domain joined** |
| Restart | Remote desktop  Remote Powershell | Remote desktop (requires further configuration)  Remote Powershell (requires further configuration)  SCCM |
| Update OS | Windows Update | Windows Update  WSUS |
| App update | Windows Store | Windows Store  SCCM |
| Skype Account Config | Not currently supported | Not currently supported |
| Access logs | Not currently supported | Not currently supported |

**Configuring Group Policy for Microsoft Teams Rooms**

This section covers system settings that Microsoft Teams Rooms depends on to function properly. When joining Microsoft Teams Rooms to a domain, ensure that your group policy doesn't override the settings in the following table.

|  |  |
| --- | --- |
| **Setting** | **Allows** |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon AutoAdminLogon = (REG\_SZ) 1 | Enables Microsoft Teams Rooms to boot up |
| Power Management -> On AC, turn screen off after 10 minutes  Power Management -> On AC, never put system to sleep | Enables Microsoft Teams Rooms to turn off attached displays and wake up automatically |
| net accounts /maxpwage:unlimited  Or equivalent means of disabling password expiration on the local account. Failure to do this will eventually cause the Skype account to fail logon complaining about an expired password. Note that this impacts all local accounts on the machine, and thus failure to set this will also cause the administrative account on the box to eventually expire as well. | Enables Skype account to always log in |

Transferring files using Group Policies is discussed in [Configure a File Item](https://technet.microsoft.com/library/cc772536%28v=ws.11%29.aspx).

**Note**

When Microsoft Teams Rooms device is compatible with the next version of Windows 10 OS, the device automatically updates to the next version through Windows Update. Microsoft Teams Rooms device should not be upgraded to next release of Windows 10 manually or via enabling Windows Update for Business (WUFB) group policies “Select the Windows readiness level for the updates you want to receive” and "Select when Preview Builds and Feature Updates are received" through GPO. A device with these group policies enabled is known to run into issues with Windows 10 OS update by Microsoft Teams Rooms app.

**Remote Management using PowerShell**

You can perform the following management operations remotely by using PowerShell (see the table below for script samples):

* Get attached devices
* Get app status
* Get system info
* Reboot system
* Retrieve logs
* Transfer files (requires a domain-joined Microsoft Teams Rooms)

**Note**

This functionality is off by default. You need to enable remote PowerShell for your environment on the Microsoft Teams Rooms system to perform the operations below. Refer to the documentation on [**Enable-PSRemoting**](https://technet.microsoft.com/library/hh849694.aspx) for information about how to enable remote PowerShell.

For example, you can enable Remote PowerShell as follows:

1. Sign in as Admin on a Microsoft Teams Rooms device.
2. Open an elevated PowerShell command prompt.
3. Enter the following command: Enable-PSRemoting -force

To perform a management operation:

1. Sign in to a PC with account credentials that have permission to run PowerShell commands on a Microsoft Teams Rooms device.
2. Open a regular PowerShell command prompt on the PC.
3. Copy the command text from the table below and paste it at the prompt.
4. Replace <Device fqdn> fields with FQDN values appropriate to your environment.
5. Replace *<path>* with the file name and local path of the master SkypeSettings.xml configuration file (or Theme image).

To Get Attached Devices

Copy

invoke-command {Write-Host "VIDEO DEVICES:"

gwmi -Class Win32\_PnPEntity | where {$\_.PNPClass -eq "Image"} | Format-Table Name,Status,Present; Write-Host "AUDIO DEVICES:"

gwmi -Class Win32\_PnPEntity | where {$\_.PNPClass -eq "Media"} | Format-Table Name,Status,Present; Write-Host "DISPLAY DEVICES:"

gwmi -Class Win32\_PnPEntity | where {$\_.PNPClass -eq "Monitor"} | Format-Table Name,Status,Present} -ComputerName <Device fqdn>

Get App Status

Copy

invoke-command { $package = get-appxpackage -User Skype -Name Microsoft.SkypeRoomSystem; if ($package -eq $null) {Write-host "SkypeRoomSystems not installed."} else {write-host "SkypeRoomSystem Version : " $package.Version}; $process = Get-Process -Name "Microsoft.SkypeRoomSystem" -ErrorAction SilentlyContinue; if ($process -eq $null) {write-host "App not running."} else {$process | format-list StartTime,Responding}} -ComputerName <Device fqdn>

Get System Info

Copy

invoke-command {gwmi -Class Win32\_ComputerSystem | Format-List PartOfDomain,Domain,Workgroup,Manufacturer,Model

gwmi -Class Win32\_Bios | Format-List SerialNumber,SMBIOSBIOSVersion} -ComputerName <Device fqdn>

Reboot System

Copy

invoke-command { Shutdown /r /t 0 } -ComputerName <Device fqdn>

Retrieve Logs

Copy

$targetDevice = "<Device fqdn> "

$logFile = invoke-command {$output = Powershell.exe -ExecutionPolicy Bypass -File C:\Rigel\x64\Scripts\Provisioning\ScriptLaunch.ps1 CollectSrsV2Logs.ps1

Get-ChildItem -Path C:\Rigel\\*.zip | Sort-Object -Descending -Property LastWriteTime | Select-Object -First 1} -ComputerName $targetDevice

$session = new-pssession -ComputerName $targetDevice

Copy-Item -Path $logFile.FullName -Destination .\ -FromSession $session; invoke-command {remove-item -force C:\Rigel\\*.zip} -ComputerName $targetDevice

Push an XML configuration file (or theme graphic)

Copy

$movefile = "<path>";

$targetDevice = "\\<Device fqdn> \Users\Skype\AppData\Local\Packages\Microsoft.SkypeRoomSystem\_8wekyb3d8bbwe\LocalState\SkypeSettings.xml";

Copy-Item $movefile $targetDevice

**Software updates**

By default, Microsoft Teams Rooms attempts to connect to the Windows Store to get the latest version of Microsoft Teams Rooms software, so the device will require regular internet access. Before contacting Microsoft with support issues, be sure the Microsoft Teams Rooms device is loaded with the latest version of the app.

By default, Microsoft Teams Rooms connects to Windows Update to retrieve operating system and USB peripheral device firmware updates, and installs them outside of configured business hours. You can configure business hours by signing into the administrator account and running the Settings app.

If you want to manage updates manually, and are unable to follow the normal procedure for [Microsoft Store for Business](https://businessstore.microsoft.com/store) to [Distribute offline apps](https://docs.microsoft.com/microsoft-store/distribute-offline-apps), you can acquire the appropriate APPX file and dependencies from the [deployment kit](https://go.microsoft.com/fwlink/?linkid=851168) (from the instructions to [Configure a Microsoft Teams Rooms console](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console)) that can be used with SCCM. The deployment kit release lags behind the store release, so it might not always match the latest available build.

**To update using Powershell**

1. Extract the package from the installation [MSI](https://go.microsoft.com/fwlink/?linkid=851168) to a share the device can access.
2. Run the following script targeting the Microsoft Teams Rooms devices, changing <share> to the device share as appropriate:

Copy

Add-AppxPackage -Update -ForceApplicationShutdown -Path '\\<share>\$oem$\$1\Rigel\x64\Ship\AppPackages\\*\\*.appx' -DependencyPath (Get-ChildItem '\\<share>\$oem$\$1\Rigel\x64\Ship\AppPackages\\*\Dependencies\x64\\*.appx' | Foreach-Object {$\_.FullName})

**Admin mode and device management**

Some management functions, like manually installing a private CA certificate, require placing the Surface Pro device in Admin mode.

**Switching to Admin Mode and back when the Microsoft Teams Rooms app is running**

1. Hang up any ongoing calls, and return to the home screen.
2. Select the Gear icon and bring up the menu (options are **Settings**, **Accessibility**, and **Restart Device** ).
3. Select **Settings**.
4. Enter the Administrator Password. The Setup screen will appear.  
     **Note** If the device isn't domain-joined, the local administrative account (username "Admin") will be used by default. The default password for this account is 'sfb' but it is recommended that your organization change this for security reasons as soon as possible. If the machine is domain-joined, you can sign in with an appropriately privileged domain account.
5. Select **Windows Settings** in the left column.
6. Choose **Go to Admin Sign-in**.
7. Enter the Administrator Password. This will gracefully log off the app and take you to the Windows login screen.
8. Log in to the desktop with your administrative credentials. You'll have the necessary privileges to manage the device.
9. Perform the necessary administrative tasks.
10. Sign out from the Admin account.
11. Return to Microsoft Teams Rooms by selecting the user account icon on the far left side of the screen and then selecting **Skype**.  
     If the **Skype** user is not listed, you might have to select **other user** and enter **.\skype** as the user name, and sign in.

The console is now back in its normal operation mode.The following procedure requires you to attach a keyboard to the device if one is not already attached.

**Switching to Admin Mode and back when the Microsoft Teams Rooms app crashes**

1. Press the Windows key five times in rapid succession. This will bring you to the Windows logon screen.
2. Log in to the desktop with your administrative credentials.  
     **Note** This method doesn't log the Skype user off or gracefully terminate the app, but you'd use it if the app wasn't responding and the other method wasn't available.
3. Perform the necessary administrative tasks.
4. Restart the machine when you're finished.  
    The console restarts into its normal operation mode, running the Microsoft Teams Rooms app. You can remove the keyboard, if it was attached to allow you to perform this procedure.  
    **Troubleshooting tips**

* Meeting invitations might not appear when sent across domain boundaries (for example, between two companies). In such cases, IT admins should decide whether to allow external users to schedule a meeting.
* Microsoft Teams Rooms doesn't support Exchange AutoDiscover redirects via Exchange 2010.
* In general, it's a good practice for IT admins to disable any audio endpoints they don't intend to use.
* In the event that a mirror image is displayed in room preview, the IT admin can correct by cycling camera power or flipping the image orientation using the camera remote control.
* Loss of console touchscreen access has been known to occur. In such cases, the issue is sometimes resolved by restarting the Microsoft Teams Rooms system.
* Loss of local audio when connecting a PC to console via wired ingest has been known to occur. In such cases, restarting the PC can resolve the local audio playback issue.

**Microsoft Teams Rooms maintenance and operations**

Read this topic to learn about management of Microsoft Teams Rooms, the next generation of Skype Room Systems.

Microsoft Teams Rooms is Microsoft's latest conferencing solution designed to transform your meeting room into a rich, collaborative experience. Users will enjoy its familiar Microsoft Teams or Skype for Business interface and IT administrators will appreciate an easily deployed and managed Windows 10 Skype Meeting app. Microsoft Teams Rooms is designed to leverage existing equipment like LCD panels for ease of installation to bring Microsoft Teams or Skype for Business into your meeting room.

With additional configuration, remote management is possible using Microsoft Azure Monitor as described in [Plan Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-plan), [Deploy Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy), [Manage Microsoft Teams Rooms devices with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy). You may also [Manage Microsoft Teams Rooms console settings remotely with an XML configuration file](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/xml-config-file), which includes applying a Custom display theme.

**Collecting logs on Microsoft Teams Rooms**

To collect logs, you must invoke the log collection script that ships with the Microsoft Teams Rooms app. In Admin mode, start an elevated command prompt, and issue the following command:

Copy

powershell -ExecutionPolicy unrestricted c:\rigel\x64\scripts\provisioning\ScriptLaunch.ps1 CollectSrsV2Logs.ps1

The logs will be output as a ZIP file in c:\rigel.

**Front of Room Display Settings**

Configure the Front of Room display to Extended mode. Doing so will ensure that the console UI is not duplicated on that display when you cycle power on the display.

**Note**

A consumer TV used as a front of room display needs to support/enable the Consumer Electronics Control (CEC) feature of HDMI so that it can switch automatically to an active video source from standby mode. This feature is not supported on all TVs.

**Microsoft Teams Rooms Reset (Factory Restore)**

If Microsoft Teams Rooms isn't running well, performing a factory reset might help. This can be done in the Settings app on the **Recovery** tab. Beneath **Reset this PC**, select **Get started**, and then **Remove everything**. Follow the remaining prompts to reset the device.

**Note**

There is a known issue where the Microsoft Teams Rooms can become unusable if the **Keep my files - Removes Apps and settings, but keeps your personal files** option is selected during the Windows Reset process. Do *not* use this option.

**Supported Remote Options**

The following table summarizes the possible remote operations and the methods you can use to accomplish them.

|  |  |  |
| --- | --- | --- |
| **Workgroup** | **Not domain joined** | **Domain joined** |
| Restart | Remote desktop  Remote Powershell | Remote desktop (requires further configuration)  Remote Powershell (requires further configuration)  SCCM |
| Update OS | Windows Update | Windows Update  WSUS |
| App update | Windows Store | Windows Store  SCCM |
| Skype Account Config | Not currently supported | Not currently supported |
| Access logs | Not currently supported | Not currently supported |

**Configuring Group Policy for Microsoft Teams Rooms**

This section covers system settings that Microsoft Teams Rooms depends on to function properly. When joining Microsoft Teams Rooms to a domain, ensure that your group policy doesn't override the settings in the following table.

|  |  |
| --- | --- |
| **Setting** | **Allows** |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon AutoAdminLogon = (REG\_SZ) 1 | Enables Microsoft Teams Rooms to boot up |
| Power Management -> On AC, turn screen off after 10 minutes  Power Management -> On AC, never put system to sleep | Enables Microsoft Teams Rooms to turn off attached displays and wake up automatically |
| net accounts /maxpwage:unlimited  Or equivalent means of disabling password expiration on the local account. Failure to do this will eventually cause the Skype account to fail logon complaining about an expired password. Note that this impacts all local accounts on the machine, and thus failure to set this will also cause the administrative account on the box to eventually expire as well. | Enables Skype account to always log in |

Transferring files using Group Policies is discussed in [Configure a File Item](https://technet.microsoft.com/library/cc772536%28v=ws.11%29.aspx).

**Note**

When Microsoft Teams Rooms device is compatible with the next version of Windows 10 OS, the device automatically updates to the next version through Windows Update. Microsoft Teams Rooms device should not be upgraded to next release of Windows 10 manually or via enabling Windows Update for Business (WUFB) group policies “Select the Windows readiness level for the updates you want to receive” and "Select when Preview Builds and Feature Updates are received" through GPO. A device with these group policies enabled is known to run into issues with Windows 10 OS update by Microsoft Teams Rooms app.

**Remote Management using PowerShell**

You can perform the following management operations remotely by using PowerShell (see the table below for script samples):

* Get attached devices
* Get app status
* Get system info
* Reboot system
* Retrieve logs
* Transfer files (requires a domain-joined Microsoft Teams Rooms)

**Note**

This functionality is off by default. You need to enable remote PowerShell for your environment on the Microsoft Teams Rooms system to perform the operations below. Refer to the documentation on [**Enable-PSRemoting**](https://technet.microsoft.com/library/hh849694.aspx) for information about how to enable remote PowerShell.

For example, you can enable Remote PowerShell as follows:

1. Sign in as Admin on a Microsoft Teams Rooms device.
2. Open an elevated PowerShell command prompt.
3. Enter the following command: Enable-PSRemoting -force

To perform a management operation:

1. Sign in to a PC with account credentials that have permission to run PowerShell commands on a Microsoft Teams Rooms device.
2. Open a regular PowerShell command prompt on the PC.
3. Copy the command text from the table below and paste it at the prompt.
4. Replace <Device fqdn> fields with FQDN values appropriate to your environment.
5. Replace *<path>* with the file name and local path of the master SkypeSettings.xml configuration file (or Theme image).

To Get Attached Devices

Copy

invoke-command {Write-Host "VIDEO DEVICES:"

gwmi -Class Win32\_PnPEntity | where {$\_.PNPClass -eq "Image"} | Format-Table Name,Status,Present; Write-Host "AUDIO DEVICES:"

gwmi -Class Win32\_PnPEntity | where {$\_.PNPClass -eq "Media"} | Format-Table Name,Status,Present; Write-Host "DISPLAY DEVICES:"

gwmi -Class Win32\_PnPEntity | where {$\_.PNPClass -eq "Monitor"} | Format-Table Name,Status,Present} -ComputerName <Device fqdn>

Get App Status

Copy

invoke-command { $package = get-appxpackage -User Skype -Name Microsoft.SkypeRoomSystem; if ($package -eq $null) {Write-host "SkypeRoomSystems not installed."} else {write-host "SkypeRoomSystem Version : " $package.Version}; $process = Get-Process -Name "Microsoft.SkypeRoomSystem" -ErrorAction SilentlyContinue; if ($process -eq $null) {write-host "App not running."} else {$process | format-list StartTime,Responding}} -ComputerName <Device fqdn>

Get System Info

Copy

invoke-command {gwmi -Class Win32\_ComputerSystem | Format-List PartOfDomain,Domain,Workgroup,Manufacturer,Model

gwmi -Class Win32\_Bios | Format-List SerialNumber,SMBIOSBIOSVersion} -ComputerName <Device fqdn>

Reboot System

Copy

invoke-command { Shutdown /r /t 0 } -ComputerName <Device fqdn>

Retrieve Logs

Copy

$targetDevice = "<Device fqdn> "

$logFile = invoke-command {$output = Powershell.exe -ExecutionPolicy Bypass -File C:\Rigel\x64\Scripts\Provisioning\ScriptLaunch.ps1 CollectSrsV2Logs.ps1

Get-ChildItem -Path C:\Rigel\\*.zip | Sort-Object -Descending -Property LastWriteTime | Select-Object -First 1} -ComputerName $targetDevice

$session = new-pssession -ComputerName $targetDevice

Copy-Item -Path $logFile.FullName -Destination .\ -FromSession $session; invoke-command {remove-item -force C:\Rigel\\*.zip} -ComputerName $targetDevice

Push an XML configuration file (or theme graphic)

Copy

$movefile = "<path>";

$targetDevice = "\\<Device fqdn> \Users\Skype\AppData\Local\Packages\Microsoft.SkypeRoomSystem\_8wekyb3d8bbwe\LocalState\SkypeSettings.xml";

Copy-Item $movefile $targetDevice

**Software updates**

By default, Microsoft Teams Rooms attempts to connect to the Windows Store to get the latest version of Microsoft Teams Rooms software, so the device will require regular internet access. Before contacting Microsoft with support issues, be sure the Microsoft Teams Rooms device is loaded with the latest version of the app.

By default, Microsoft Teams Rooms connects to Windows Update to retrieve operating system and USB peripheral device firmware updates, and installs them outside of configured business hours. You can configure business hours by signing into the administrator account and running the Settings app.

If you want to manage updates manually, and are unable to follow the normal procedure for [Microsoft Store for Business](https://businessstore.microsoft.com/store) to [Distribute offline apps](https://docs.microsoft.com/microsoft-store/distribute-offline-apps), you can acquire the appropriate APPX file and dependencies from the [deployment kit](https://go.microsoft.com/fwlink/?linkid=851168) (from the instructions to [Configure a Microsoft Teams Rooms console](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/console)) that can be used with SCCM. The deployment kit release lags behind the store release, so it might not always match the latest available build.

**To update using Powershell**

1. Extract the package from the installation [MSI](https://go.microsoft.com/fwlink/?linkid=851168) to a share the device can access.
2. Run the following script targeting the Microsoft Teams Rooms devices, changing <share> to the device share as appropriate:

Copy

Add-AppxPackage -Update -ForceApplicationShutdown -Path '\\<share>\$oem$\$1\Rigel\x64\Ship\AppPackages\\*\\*.appx' -DependencyPath (Get-ChildItem '\\<share>\$oem$\$1\Rigel\x64\Ship\AppPackages\\*\Dependencies\x64\\*.appx' | Foreach-Object {$\_.FullName})

**Admin mode and device management**

Some management functions, like manually installing a private CA certificate, require placing the Surface Pro device in Admin mode.

**Switching to Admin Mode and back when the Microsoft Teams Rooms app is running**

1. Hang up any ongoing calls, and return to the home screen.
2. Select the Gear icon and bring up the menu (options are **Settings**, **Accessibility**, and **Restart Device** ).
3. Select **Settings**.
4. Enter the Administrator Password. The Setup screen will appear.  
     **Note** If the device isn't domain-joined, the local administrative account (username "Admin") will be used by default. The default password for this account is 'sfb' but it is recommended that your organization change this for security reasons as soon as possible. If the machine is domain-joined, you can sign in with an appropriately privileged domain account.
5. Select **Windows Settings** in the left column.
6. Choose **Go to Admin Sign-in**.
7. Enter the Administrator Password. This will gracefully log off the app and take you to the Windows login screen.
8. Log in to the desktop with your administrative credentials. You'll have the necessary privileges to manage the device.
9. Perform the necessary administrative tasks.
10. Sign out from the Admin account.
11. Return to Microsoft Teams Rooms by selecting the user account icon on the far left side of the screen and then selecting **Skype**.  
     If the **Skype** user is not listed, you might have to select **other user** and enter **.\skype** as the user name, and sign in.

The console is now back in its normal operation mode.The following procedure requires you to attach a keyboard to the device if one is not already attached.

**Switching to Admin Mode and back when the Microsoft Teams Rooms app crashes**

1. Press the Windows key five times in rapid succession. This will bring you to the Windows logon screen.
2. Log in to the desktop with your administrative credentials.  
     **Note** This method doesn't log the Skype user off or gracefully terminate the app, but you'd use it if the app wasn't responding and the other method wasn't available.
3. Perform the necessary administrative tasks.
4. Restart the machine when you're finished.  
    The console restarts into its normal operation mode, running the Microsoft Teams Rooms app. You can remove the keyboard, if it was attached to allow you to perform this procedure.  
    **Troubleshooting tips**

* Meeting invitations might not appear when sent across domain boundaries (for example, between two companies). In such cases, IT admins should decide whether to allow external users to schedule a meeting.
* Microsoft Teams Rooms doesn't support Exchange AutoDiscover redirects via Exchange 2010.
* In general, it's a good practice for IT admins to disable any audio endpoints they don't intend to use.
* In the event that a mirror image is displayed in room preview, the IT admin can correct by cycling camera power or flipping the image orientation using the camera remote control.
* Loss of console touchscreen access has been known to occur. In such cases, the issue is sometimes resolved by restarting the Microsoft Teams Rooms system.
* Loss of local audio when connecting a PC to console via wired ingest has been known to occur. In such cases, restarting the PC can resolve the local audio playback issue.

**Manage Microsoft Teams Rooms devices with Azure Monitor**

This article discusses how to manage Microsoft Teams Rooms devices in an integrated, end-to-end manner using Azure Monitor.

You can configure Azure Monitor to provide basic telemetry that will help you manage Skype meeting room devices (see [Plan Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-plan) and [Deploy Microsoft Teams Rooms management with Azure Monitor]((azure-monitor-deploy.md) for details). As your management solution matures, you can use additional data and management capabilities to create a more detailed view of device performance.

**Understand the log entries**

The following event descriptions are inserted into the event log description field every five minutes, when the Microsoft Teams Room app records the corresponding information in the Windows event log. The Microsoft Monitoring Agent passes these records to Log Analytics in Azure Monitor, which parses them into the dashboard you created in [Deploy Microsoft Teams Rooms management with Azure Monitor](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/azure-monitor-deploy). Using the dashboard you can look at individual log entries to determine courses of action if needed.

Event IDs 2000 and 3000 indicate the device in question is working as expected. Event IDs 2001 and 3001 indicate an issue was found. Event ID 4000 may require action if it is seen more often than you expect, compared to a baseline you set or other deployed devices in your organization.

Understanding these event descriptions alerts you to problems quickly, and provides a starting point for further troubleshooting.

|  |  |  |
| --- | --- | --- |
| **Event ID level** | **Event behavior** | **Event Description** |
| 2000  Information | This is a healthy heartbeat event. Every 5 minutes, Microsoft Teams Rooms checks that it is signed in to Microsoft Teams or Skype for Business and has network and Exchange connectivity.  If all 3 factors are true, it will write Event ID 2000 into the event log every 5 minutes until the device is offline or one or more of the conditions is no longer met. | {"Description":"Heartbeat is healthy.", "ResourceState":"Healthy", "OperationName":"Heartbeat", "OperationResult":"Pass", "OS":"Windows 10", "OSVersion":"10.0.14393.693", "Alias":"alias@contoso.com", "DisplayName":"Display name", "AppVersion":"1.0.38.0", "IPv4Address":"10.10.10.10", "IPv6Address":"IP v6 address"}  In this example, all heartbeat conditions were met and the Microsoft Teams Rooms device was marked as being healthy. If there were errors, the app would record Event ID 2001 instead. |
| 2001  Error | This is an app error event. Every 5 minutes, Microsoft Teams Rooms checks that it is signed in to Microsoft Teams or Skype for Business with network and Exchange connectivity. If one or more factors are not true, it will write EventID 2001 into the event log every 5 minutes until the device is offline or all of the conditions are able to be met once again. | {"Description":"Network status : Healthy. Exchange status : Connected. **Signin status: Unhealthy.** ", "ResourceState":"Unhealthy", "OperationName":"Heartbeat", "OperationResult":"Fail", "OS":"Windows 10", "OSVersion":"10.0.14393.693", "Alias":"", "DisplayName":"Display Name", "AppVersion":"1.0.38.0", "IPv4Address":"10.10.10.10", "IPv6Address":"ip v6 address"}  In this example, Microsoft Teams Rooms determined that the network connection was healthy and the app was connected to Exchange, but the bolded portion indicates the app is not connected to Skype for Business. This could be a configuration issue on the device or host.  The Network status will show as either Healthy or Unhealthy. If the status is unhealthy, you may have a network issue or the device may have been unplugged (but then you would probably also have Exchange and Microsoft Teams or Skype for Business errors).  The Exchange Status will show as either Connected or one of the following: Disconnected, Connecting, AutodiscoveryError (the most commonly seen error), GeneralError, or ServerVersionNotSupported. If the status is Connecting, wait until the next health message is sent, for other errors refer the issue to an admin with experience in solving Exchange issues.  The Signin status (indicating the app is signed in to Skype for Business) will show as either Healthy or Unhealthy. If the status is unhealthy, send a technician to investigate further. |
| 3000  Information | This event verifies that a hardware check was run and found to be healthy. Every 5 minutes Microsoft Teams Rooms checks that configured hardware components such as front of room display, microphone, speaker, and camera are connected and functioning. If all components are healthy, it will write EventID 3000 into the event log. This event will continue to be written every 5 minutes unless there is an issue with a connected device. | {"Description":"HardwareCheckEngine is healthy.", "ResourceState":"Healthy", "OperationName":"HardwareCheckEngine", "OperationResult":"Pass", "OS":"Windows 10", "OSVersion":"10.0.14393.693", "Alias":"alias@contoso.com", "DisplayName":"Display Name", "AppVersion":"1.0.38.0", "IPv4Address":"10.10.10.10", "IPv6Address":"ip v6 address"}  In this example, all hardware checks were passed. If there were errors, the app would record Event ID 3001 instead. |
| 3001  Error Event | This is a hardware error event. The Microsoft Teams Rooms app has a process that will check the health of connected hardware components (front of room, microphone, speaker, camera) every 5 minutes. If one or more of the components are unhealthy, it will write EventID 3001 into the event log. This event will continue to be written every 5 minutes until the issue with the device is fixed. | {"Description":" **Front of Room Display status : Unhealthy.** Configured display count is 2. Real display count is 0. **Conference Microphone status : Unhealthy.** Conference Speaker status : Healthy. Default Speaker status : Healthy. Camera status : Healthy.", "ResourceState":"Unhealthy", "OperationName":"HardwareCheckEngine", "OperationResult":"Fail", "OS":"Windows 10", "OSVersion":"10.0.14393.1198", "Alias":"alias@contoso.com", "DisplayName":"Yosemite conference room", "AppVersion":"2.0.58.0", "IPv4Address":"10.10.10.10", "IPv6Address":"IPv6Address", "IPv4Address2":"10.10.10.10"}  Hardware peripherals are shown as either Healthy or Unhealthy.  In this example, there are two front of room displays configured, and currently neither of them is available. The Conference Microphone status is unhealthy, which could have a number of possible causes. Since at least one resource did not pass the check, the ResourceState is listed as Unhealthy. Send a technician to investigate further. |
| 4000  Information | This is an App Restart event. Every time the app is restarted, it will log this event into the Windows event log. | {"Description":"App restarts.", "ResourceState":"Healthy", "OperationName":"Restart", "OperationResult":"Pass", "OS":"Windows 10", "OSVersion":"10.0.14393.693", "Alias":"alias@domain.com", "DisplayName":"Display Name", "AppVersion":"1.0.38.0", "IPv4Address":"10.10.10.10", "IPv6Address":"ip v6 address"}  The app may restart for a variety of reasons. compare the restart frequency of devices in the same building and in different buildings, keeping in mind known issues like power fluctuations and failures, as this may provide clues to infrastructure problems. |

**Manage a Microsoft Teams Rooms console settings remotely with an XML configuration file**

This article discusses remote management of the default settings used by a Microsoft Teams Rooms device, including applying a custom theme.

Updating a master XML file and sending copies to the consoles you manage makes it possible for you to change default settings for remotely managed devices. This article discusses how to create such a file, and links to discussions of how to place them as needed on the remotely managed devices. Using this method, you can also implement Custom Themes on your Microsoft Teams Rooms consoles.

**Creating an XML configuration file**

The table below explains the elements shown in this sample SkypeSettings.xml (this is a required file name) configuration file.

Copy

<SkypeSettings>

<AutoScreenShare>true</AutoScreenShare>

<HideMeetingName>true</HideMeetingName>

<UserAccount>

<SkypeSignInAddress>RanierConf@contoso.com</SkypeSignInAddress>

<ExchangeAddress>RanierConf@contoso.com</ExchangeAddress>

<DomainUsername>Seattle\RanierConf</DomainUsername>

<Password>password</Password>

<ConfigureDomain>domain1, domain2</ConfigureDomain>

</UserAccount>

<IsTeamsDefaultClient>false</IsTeamsDefaultClient>

<BluetoothAdvertisementEnabled>true</BluetoothAdvertisementEnabled>

<SkypeMeetingsEnabled>false</SkypeMeetingsEnabled>

<TeamsMeetingsEnabled>true</TeamsMeetingsEnabled>

<DualScreenMode>true</DualScreenMode>

<SendLogs>

<EmailAddressForLogsAndFeedback>RanierConf@contoso.com</EmailAddressForLogsAndFeedback>

<SendLogsAndFeedback>true</SendLogsAndFeedback>

</SendLogs>

<Devices>

<MicrophoneForCommunication>Microsoft LifeChat LX-6000</MicrophoneForCommunication>

<SpeakerForCommunication>Realtek High Definition Audio</SpeakerForCommunication>

<DefaultSpeaker>Polycom CX5100</DefaultSpeaker>

</Devices>

<Theming>

<ThemeName>Custom</ThemeName>

<CustomThemeImageUrl>folder path</CustomThemeImageUrl>

<CustomThemeColor>

<RedComponent>100</RedComponent>

<GreenComponent>100</GreenComponent>

<BlueComponent>100</BlueComponent>

</CustomThemeColor>

</Theming>

</SkypeSettings>

If the XML file is badly formed (meaning a variable value is of the wrong type, elements are out of order, elements are unclosed, and so on), settings found up to the point where the error is found are applied, then the rest of the file is ignored during processing. Any unknown elements in the XML are ignored. If a parameter is omitted, it remains unchanged on the device. If a parameter's value is invalid, its prior value remains unchanged.

**XML elements**

|  |  |  |  |
| --- | --- | --- | --- |
| **Element** | **Type** | **Level** | **Usage** |
| <SkypeSettings> | Container for all elements. |  | Required. |
| <AutoScreenShare> | Boolean ❷ | First ❶ | If true, auto screen share is enabled. |
| <HideMeetingName> | Boolean ❷ | First ❶ | If true, meeting names are hidden. |
| <UserAccount> | Container | First ❶ | Container for credentials parameters. The sign in address, Exchange address, or email address are usually the same, such as RanierConf@contoso.com. |
| <SkypeMeetingsEnabled> | Boolean ❷ | First ❶ | Enabled by default. |
| <SkypeSignInAddress> | String ❸ |  | The sign in name for the console's Skype for Business device account. |
| <ExchangeAddress> | String ❸ |  | The sign in name for the console's Exchange device account. If the ExchangeAddress is omitted, the SkypeSignInAddress will not automatically be re-used. |
| <DomainUsername> | String ❸ |  | The domain and user name of the console device, for example Seattle\RanierConf. |
| <Password> | String 3 |  | The password parameter is the same password used for the Skype for Business device account sign-in. |
| <ConfigureDomain> | String ❸ |  | You can list several domains, separated by commas. |
| <TeamsMeetingsEnabled> | Boolean ❷ | First ❶ | Disabled by default.  The XML file is considered badly formed if both <SkypeMeetingsEnabled> and<TeamsMeetingsEnabled> are disabled, but it's acceptable to have both settings enabled at the same time. |
| <IsTeamsDefaultClient> | Boolean ❷ | First ❶ | Disabled by default. |
| <BluetoothAdvertisementEnabled> | Boolean ❷ | First ❶ | Enabled by default. |
| <DualScreenMode> | Boolean ❷ | First ❶ | If true, dual screen mode is enabled. Otherwise the device will use single screen mode. |
| <SendLogs> | Container | First ❶ |  |
| <EmailAddressForLogsAndFeedback> | String ❸ |  | This sets an optional email address that logs can be sent to when the "Give Feedback" window appears. |
| <SendLogsAndFeedback> | Boolean ❷ |  | If true, logs are sent to the admin. If false, only feedback is sent to the admin (and not logs). |
| <Devices> | Container | First ❶ | The connected audio device names in the child elements are the same values listed in the Device Manager app. The configuration can contain a device that does not presently exist on the system, such as an A/V device not currently connected to the console. The configuration would be retained for the respective device. |
| <MicrophoneForCommunication> | String ❸ |  | Sets the microphone that will be used as the recording device in a conference. |
| <SpeakerForCommunication> | String ❸ |  | Device to be used as speaker for the conference. This setting is used to set the speaker device that will be used hear the audio in a call. |
| <DefaultSpeaker> | String ❸ |  | Device to be used to play the audio from an HDMI ingest source. |
| <Theming> | Container | First ❶ | One of the features that can be applied using an XML file is a Custom Theme for your organization. You will be able to specify a theme name, background image, and color. |
| <ThemeName> | String ❸ |  | Used to identify the theme on the client. The Theme Name options are Default, one of the provided preset themes, or Custom.  Custom theme names should always use the name *Custom* . The client UI can be set at the console to the Default or one of the presets, but applying a custom theme must be set remotely by an Administrator.  Preset themes include:  Default  Blue Wave  Digital Forest  Dreamcatcher  Limeade  Pixel Perfect  Roadmap  Sunset  To disable the current theme, use "No Theme" for the ThemeName. |
| <CustomThemeImageUrl> | String ❸ |  | Required if using a custom theme, otherwise optional. See the [Custom Theme Images](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/xml-config-file#Themes) section below for more details on the custom theme image. |
| <CustomThemeColor> | Container |  | Container for the <RedComponent>, <GreenComponent>, and <BlueComponent> values. These values are required if using a custom theme. |
| <RedComponent> | Byte (0-255) |  | Represents the red color component. |
| <GreenComponent> | Byte (0-255) |  | Represents the green color component. |
| <BlueComponent> | Byte (0-255) |  | Represents the blue color component. |
|  |  |  |  |

❶ All of the first-level elements are optional. If a first-level element is omitted, all of its child parameters remain unchanged on the device.

❷ A boolean flag can be any of the following: true, false, 0, or 1. Boolean or numeric values left empty might render the XML malformed so there would be no changes to the settings.

❸ If a string parameter is present, empty, and empty is a valid value, the parameter is cleared on the device.

**Manage console settings using an XML configuration file**

At startup, if a Microsoft Teams Rooms console finds an XML file named SkypeSettings.xml at the location **C:\Users\Skype\AppData\Local\Packages\Microsoft.SkypeRoomSystem\_8wekyb3d8bbwe\LocalState**, it will apply the configuration settings indicated by the XML file then delete the XML file.

Depending on how many Microsoft Teams Rooms devices your enterprise has and how you choose to manage to configure them, there are a number of ways to place the XML configuration file. Once the file is pushed to the console, restart it to process the configuration changes. The XML configuration file is deleted after it is successfully processed. The management methods suggested for Microsoft Teams Rooms devices are discussed in:

* [Configuring Group Policy for Microsoft Teams Rooms](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-operations#GroupPolicy)
* [Remote Management using PowerShell](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/room-systems-v2-operations#RemotePS) and [Configure a File Item](https://technet.microsoft.com/library/cc772536%28v=ws.11%29.aspx)

You are free to use any method you like so long as you can use it to transfer files and trigger a restart on the console device. The file must be readable, writable, and delete-able by the device's local user account (preferably, it should be owned by and have full privileges granted to that user). If the file permissions are not set correctly, the software may fail to apply the settings, may fail to delete the file upon successful processing, and could even potentially crash.

**Custom Theme Images**

The custom theme image file must be placed in **C:\Users\Skype\AppData\Local\Packages\Microsoft.SkypeRoomSystem\_8wekyb3d8bbwe\LocalState**, just enter the file name and extension in the <CustomThemeImageUrl> variable.

The image file should be exactly 3840X1080 pixels and must be one of the following file formats: jpg, jpeg, png and bmp. If your organization wants a custom image, a graphic designer will find our [Custom Theme Photoshop Template](https://go.microsoft.com/fwlink/?linkid=870441) useful. It contains further detail on where to place various elements in a theme image and what areas appear on consoles and displays.

The XML configuration file must be updated at device startup to recognize the theme image. Once the new XML file is processed and deleted, the theme graphic file will be deleted from the directory.

**Use the Microsoft Teams Rooms recovery tool**

This article discusses how to use the recovery tool for Microsoft Teams Rooms, which you would use to bring an out of date system into a supported state. You would use this tool when the Microsoft Teams Rooms console shows a "system config out of date" error.

**Prerequisites**

Download the latest [Microsoft Teams Rooms installation package](https://go.microsoft.com/fwlink/?linkid=851168) and extract it to a USB memory stick or network share accessible to the Microsoft Teams Rooms device.

You may also need to install [KB4089848](http://download.windowsupdate.com/d/msdownload/update/software/updt/2018/03/windows10.0-kb4089848-x64_db7c5aad31c520c6983a937c3d53170e84372b11.msu).

**Verify Windows Version**

1. Login to an admin account by going to **Settings> Windows Setting> Admin Sign In** from the Microsoft Teams Rooms device. This option brings you to the login screen.
2. Sign into an admin account, the default admin account being admin with the password sfb.
3. Click on the start menu and type winver.exe into the search box and click \**Run Command*on the result.
4. Make note of the number after 'Version' on the second line of the info pane.

**Note**

If the Version shown is 1607 or earlier, follow the steps in the [**Update Windows before recovery**](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/recovery-tool#Windows-up) steps before proceding to the [**Perform a recovery**](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/recovery-tool#Perform) steps. If the Version shown is greater than 1607, follow only the steps in [**Perform a recovery**](https://docs.microsoft.com/en-us/MicrosoftTeams/room-systems/recovery-tool#Perform).

**Update Windows before recovery (if needed)**

1. While still logged in as an admin user, launch an elevated Powershell prompt.
2. Run the command Remove-Item -Path 'c:\Recovery\OEM\$oem$\$1\Rigel' -Force -Recurse.
3. Run Windows Update and install the update for Windows 1709.
4. After the update to 1709 is complete sign back into admin account and install [KB4089848](http://download.windowsupdate.com/d/msdownload/update/software/updt/2018/03/windows10.0-kb4089848-x64_db7c5aad31c520c6983a937c3d53170e84372b11.msu). The update may be done from the link or using Windows Update.
5. As an optional step, install any additional updates available from Windows Update.

**Perform a recovery**

1. Sign in to the admin account on your Microsoft Teams Rooms device, and launch an elevated command prompt.
2. Verify from the Microsoft Teams Rooms device that you are able to access the RecoveryTool.ps1 file, which is included in the files extracted from the Microsoft Teams Rooms installation package. The kit can be found on the network share or USB drive used when preparing prerequisites.
3. Run the Powershell.exe command -ExecutionPolicy Unrestricted -File "<path to RecoveryTool.ps1>".
4. When prompted by the script select option 1:"Repair System".
5. Upon completion, reboot the Microsoft Teams Rooms device. It will reboot again automatically and come up fully recovered the second time.