



## Surface Hub Adoption Training Guide: Help Desk

This page intentionally left blank

## Table of Contents

---

About This Guide .....	4
Who Should Attend? .....	4
Objectives .....	4
1. Surface Hub overview and troubleshooting.....	5
What is Surface Hub? .....	5
A Day in the Life of End Users.....	7
Device Troubleshooting.....	10
Microsoft Teams and Skype for Business meetings .....	18
2. Surface Hub configuration best practices .....	21
Device Account configuration and provisioning.....	21
Monitor device with Operations Management Suite.....	25
Walkthrough device settings and best practices.....	34
3. Manage Surface Hub updates and recovery .....	39
Setup and configure Surface Hub for Intune.....	39
Manage Windows Updates .....	44
Device Recovery and Re-configuration .....	47

## About This Guide

---

Hello and welcome to the Microsoft Surface Hub training guide. This guide includes detailed information for Surface Hub help desk as well as step-by-step troubleshooting for common issues that end users may experience during normal use. The guide can also be used as a reference after class to review the best practices for monitoring and management of Surface Hub.

## Who Should Attend?

---

This course is intended for enterprise help desk staff members who manage collaboration and audio/video devices within the organization as well as those who support end users that rely on these tools to meet with remote team members and get work done.

## Objectives

---

In this course, you will learn how to support all types of productive and collaborative work utilizing Microsoft Surface Hub. The training will not only teach you how to confidently manage and monitor Microsoft Surface Hub day-to-day, it will also show you how to configure the device to allow end users to effectively collaborate with teammates, both internally and externally. The first 2 hours are spent learning how to easily support Surface Hub every day. Then you'll learn how to apply those best practices to collaboration tools in your industry.

You will also learn about the key features of Surface Hub management including:

- **Microsoft Office/Teams Integration** – A platform for true team collaboration
- **Operations Management Suite** – Azure workspace for device monitoring and alerts
- **Device Settings** – Manage and troubleshoot issues related to your network and configuration
- **Microsoft Intune** – Remotely configure devices across your network for the optimal experience

# 1. Surface Hub overview and troubleshooting

---

## Lesson Objectives

---

After completing this lesson, you will be able to:

- Relate to the collaboration needs of end users in your organization
- Troubleshoot common issues that can arise during normal use
- Support Microsoft Teams and Skype for Business for end users

## What is Surface Hub?

---

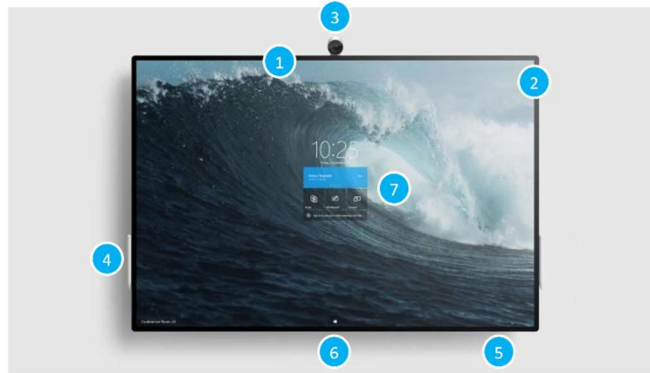
Microsoft Surface Hub 2S is the next generation team collaboration device designed to advance the way people work together naturally. Surface Hub 2S re-imagines the mobile meeting experience to unlock the power of the group by using an interactive, collaborative Whiteboard, Skype for Business, Microsoft Teams, Office apps, and Email to share content and meeting notes.



As a platform for amazing large screen apps, Surface Hub is the best way to create and brainstorm with others. In addition, since Surface Hub is a shared device, anyone can walk up and start a session from the Welcome screen. Surface Hub is advanced technology for the modern mobile workplace.

## Surface Hub Components

Surface Hub 2S includes highly refined technology with a thin bezel, light weight, and Ultra High Definition display.



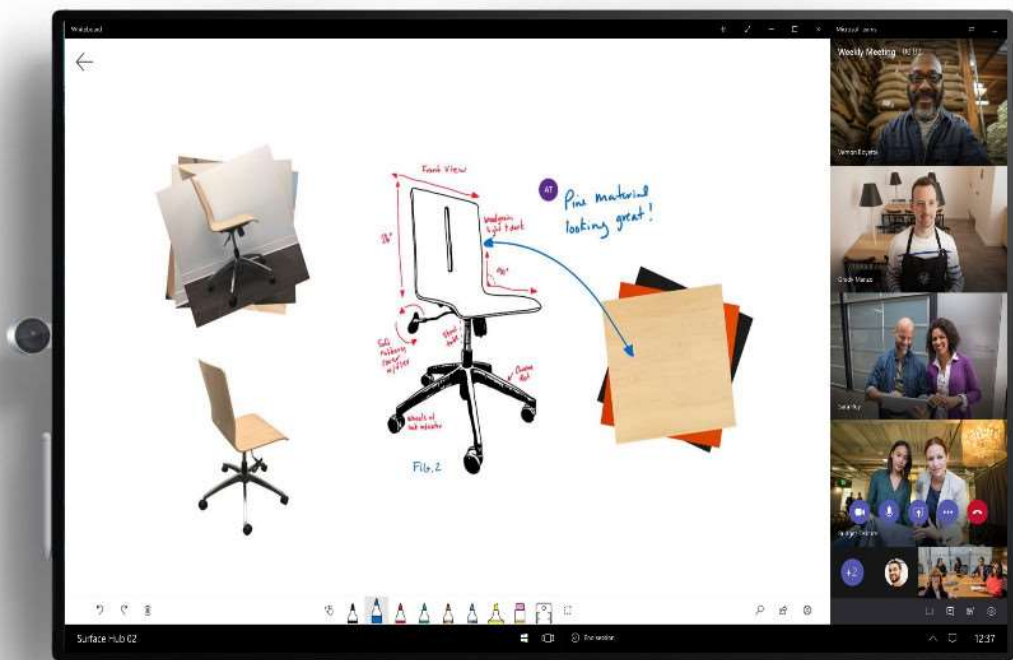
Microphone (1) and Speakers (2)	Stereo speakers and a high-quality microphone array let you converse naturally with remote participants.
Camera (3)	Surface Hub includes a high definition camera for video calling and meetings.
Pen (4)	Use the tip of the active pen to write, draw, capture, or select. Use the flat end as an eraser.
Surface buttons (5)	The buttons for Power, Volume, and Source selection are located in the bottom right of the bezel.
Ports (6)	Located on the bottom of Surface Hub are the ports for USB-A, Mini DisplayPort output, HDMI input, USB-C with DisplayPort input, and RJ45 Ethernet.
Touchscreen (7)	Use the touchscreen to open app, write or draw on the whiteboard, join a meeting, invite participants, and more.
Integrated Computer	The Surface Hub has an onboard computer that supports Microsoft Teams meetings, Microsoft Edge and Office 365 apps like Word and PowerPoint.

## A Day in the Life of End Users

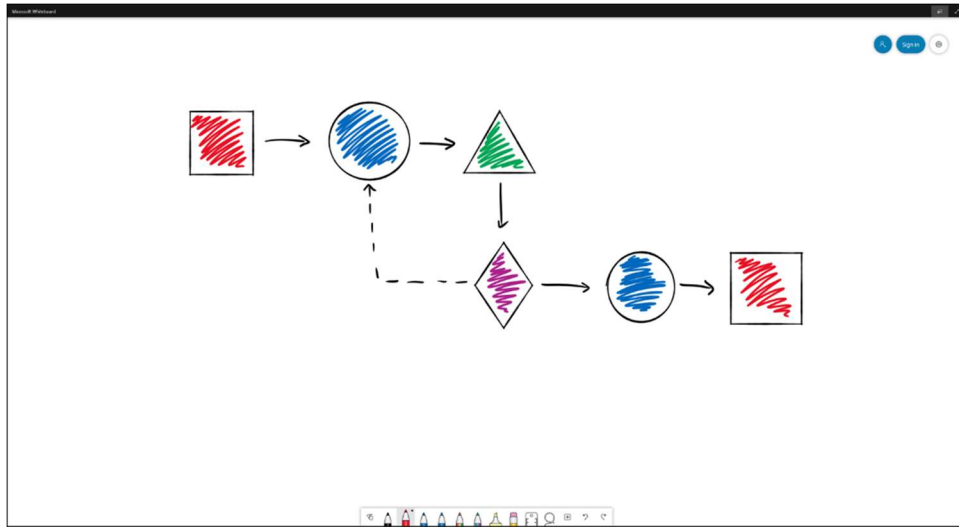
### Surface Hub collaboration

Users rely on Surface Hub every day to collaborate efficiently and work fluidly with their teams. There are many ways that Surface Hub enables teams to work and meet anywhere, turning almost any space into a collaboration space.

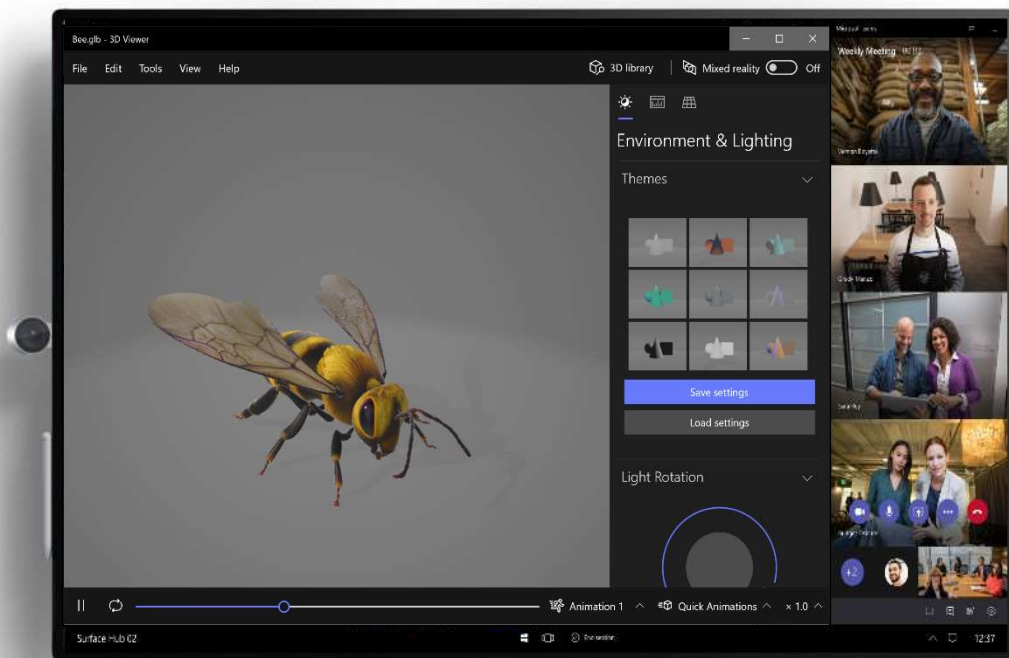
**Teams video calls and scheduled meetings** let users work face to face with colleagues no matter where they are.



**An infinite canvas Whiteboard** allows users to brainstorm without limits and share creativity with anyone in the organization.

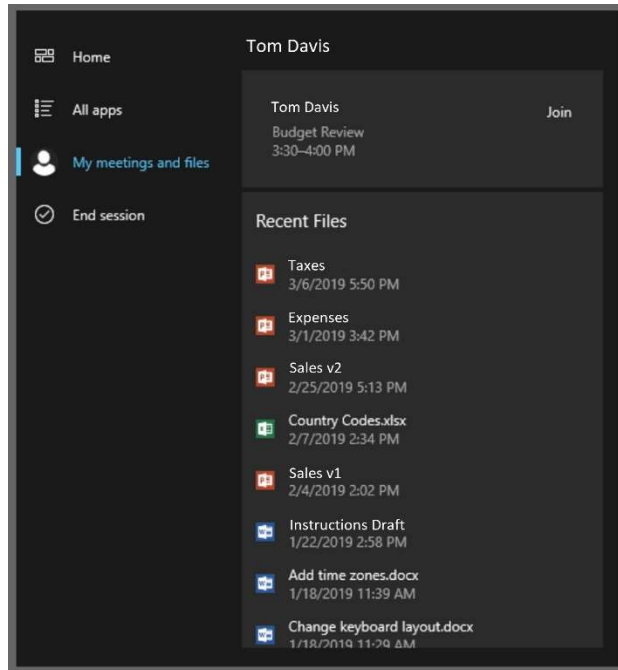


**Wireless projection with touchback** provides instant large screen access to any Windows application for engaging meetings and presentations.

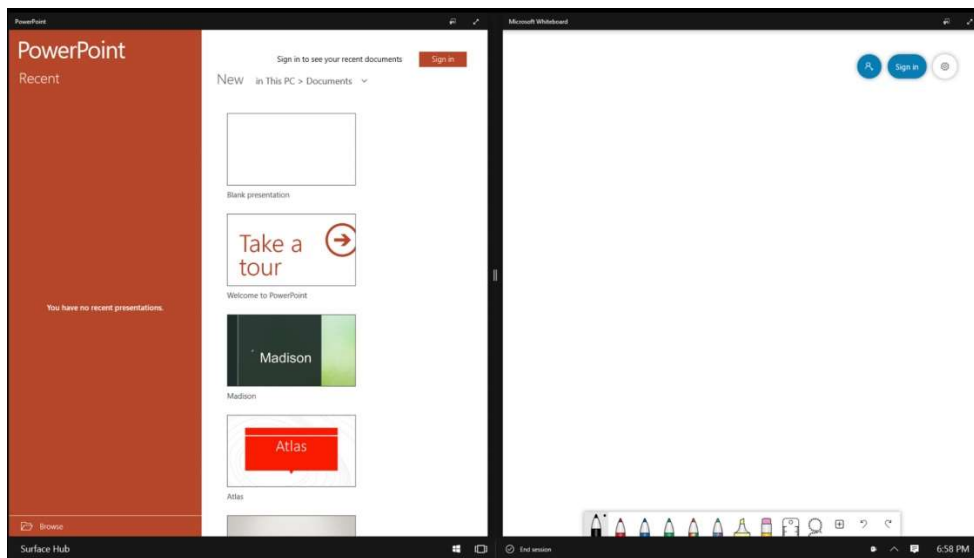




**Office 365 apps and access** gives everyone a mobile access point to all of their content and their meeting calendar.



**Multitasking with large screen apps** helps meetings become more efficient and productive.



Maintaining Surface Hub in a ready state for any user to be able to walk up and start using it for all of their collaboration needs is one of the key tasks of the Help Desk role. Its important to understand the various tasks that users may perform on Surface Hub and how those features can be impacted adversely by improper maintenance, lack of updates, network availability, and access to resources and services.

## Device Troubleshooting

---

### Troubleshooting apps and device features

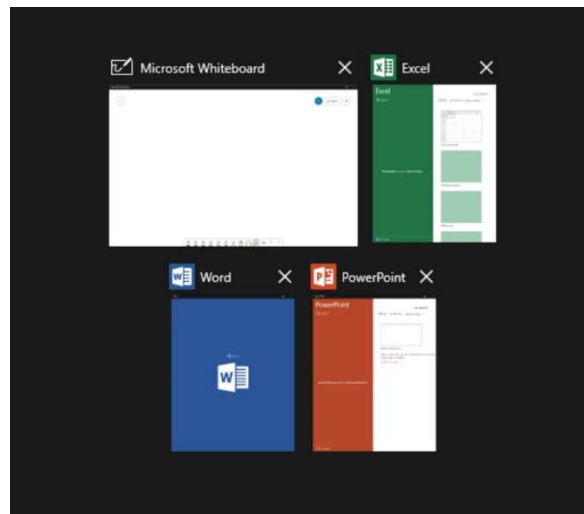
Getting work done with Surface Hub is easier than ever with multitasking and video conferencing at your fingertips. There are some simple ways to keep everything running optimally for end users.

Remember to always save your work. The best way to make sure your work is saved is to utilize Office 365 and Microsoft OneDrive for file access. While users are signed in to Office 365, files and whiteboards will be saved automatically to their profile.

### Restart apps

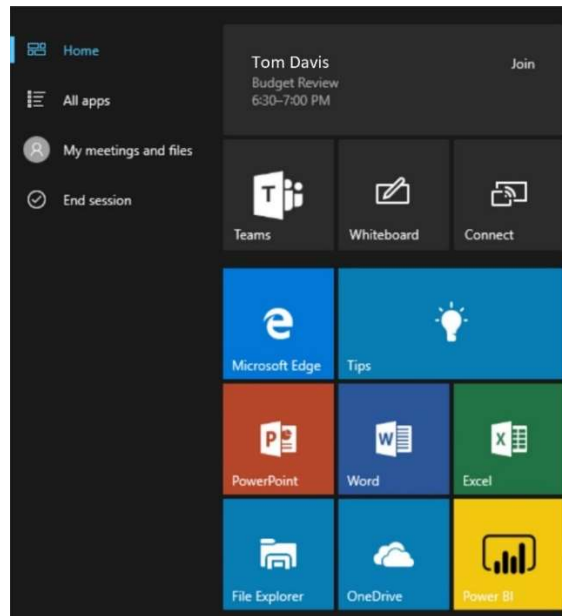
During normal use, an app on Surface Hub may not behave as users expect. The quickest way to fix an issue with a specific app is to close the app as well as any other unneeded apps using Task View and re-launch the app from the Start menu.

Press the **Task View** button to display all running apps, including those that may be running in the background.



Press the **x** to close any apps you no longer need as well as the app that isn't behaving as expected.

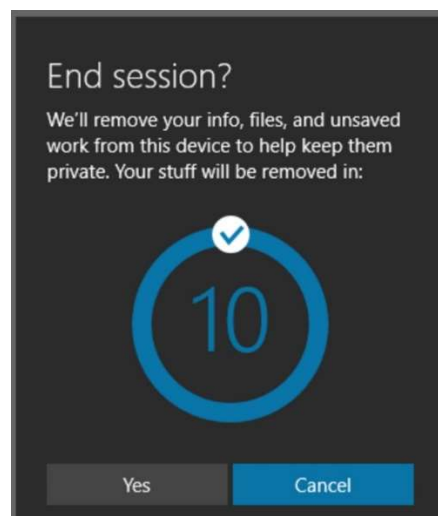
Open the **Start Menu** to re-launch any apps that you need. As long as you saved your work, you can continue right where you left off.



## End Session

Surface Hub is designed to provide users with the same fresh experience for every session. The best way to start with a fresh session is to save all work and end the session. This can be helpful if you want to reset for the next group or just need a fresh start.

Press **End Session** to display the 10-second countdown timer.



If you need to cancel the countdown for any reason, tap anywhere else on the screen or press **Cancel**.

To skip the countdown and immediately end the session, press the **Check** mark or press **Yes**.

After a few seconds the welcome screen will appear and get ready for the next session.

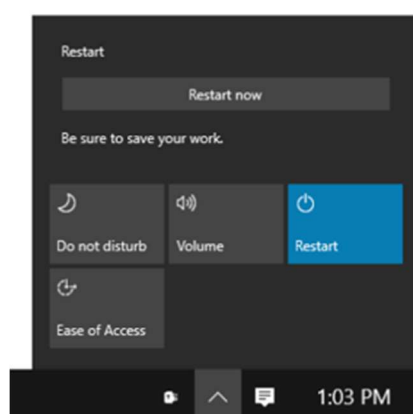
## Restart

Before you restart Surface Hub make sure you have saved any work you need.

To restart Surface Hub press the ^ menu in the bottom right corner of the screen.

In the menu, select **Restart**.

Then select **Restart Now**. Keep in mind that there is no 10-second countdown, the device will immediately restart which means any unsaved work will be lost.



## Power off/on

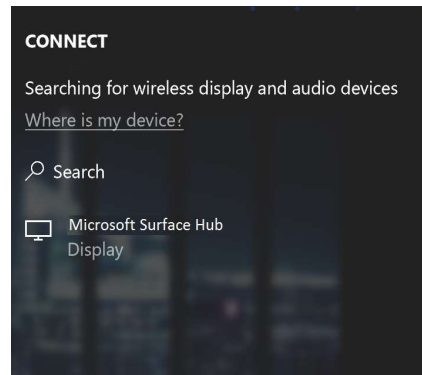
To power off a Surface Hub, press the Power button located on the bottom of the device. Then unplug the device from the wall and the battery (if connected). Wait about 10 seconds and then plug the power back into the device. This will cause the device to turn on and boot up to the Welcome screen.

## Troubleshooting connected devices

There are several ways to connect devices to Surface Hub to bring in content for meetings and collaboration. Surface Hub supports both wireless and wired connections.

Miracast provides is a wireless connection between two devices. Surface Hub listens for incoming connections via Miracast which is available built into Windows 10. As long as your hardware device supports Miracast and runs Windows 10, you should be able to wirelessly project your screen onto Surface Hub.

On your laptop, press **Windows + K** to bring up the Connect pane and look for the friendly name of the Surface Hub which will be displayed in the bottom left corner of the screen.



If the connection fails there are several settings that should be verified along with the hardware on the connecting device.

On the Surface Hub, open **Settings**. Then check the network settings to make sure the WiFi is enabled. Surface Hub doesn't need to be connected to a wireless network, but it does need to be enabled in order for Miracast to work.

Also verify that Miracast projection is enabled. In Settings, select **Surface Hub > Projection** to make sure that Projection is enabled. If a PIN is required make a note of that setting as well, since the first time a device connects it will require they enter the PIN on their device.

The network hardware on the laptop must also support Miracast and may require a driver update first.

If Miracast has worked at some point but fails intermittently, try restarting both the laptop and Surface Hub to reset the connection and try again.

Some mobile devices also support Miracast, check with the device manufacturer to determine if Miracast is supported.

### Advanced Miracast Troubleshooting

Surface Hub supports wireless projection through the Miracast protocol. Most wireless monitors and adapters available today use the original implementation of Miracast. Surface Hub uses a slightly different version of Miracast known as Miracast Autonomous Group Owner (AGO). A common troubleshooting step when projecting wirelessly to Surface Hub fails is to test projecting to another wireless monitor or adapter. However, in most cases, these devices are not using Miracast AGO and do not handle wireless projection the same way that Surface Hub does.

In traditional Miracast, the projecting device will connect the access point set up by the Miracast-enabled monitor, and then the monitor will send traffic back to the projecting device using the network channel of the projecting device.

Miracast AGO is a two-step connection process:

The first step is an initial connection using 2.4GHz.

After that initial handshake, the projecting device sends traffic to the monitor using the wireless channel settings on the monitor. If Surface Hub is connected to a Wi-Fi network, the access point, it will use the same channel as the connected network, otherwise it will use the Miracast channel from Settings.

There are generally two types of issues with Miracast to Surface Hub: connection and performance. In either case, it is a good idea to get a general picture of wireless network activity in the Surface Hub's location. Running a network scanning tool will show you the available networks and channel usage in the environment.

### *Connection*

If you ran a network scan, you should see Surface Hub Miracast listed as an access point. If Surface Hub's Miracast network shows up on the scan, but you cannot not see it as an available device, you can try to adjust the Miracast channel used by Surface Hub.

When Surface Hub is connected to a Wi-Fi network it will use the same channel settings as the Wi-Fi access point for its Miracast access point. For troubleshooting purposes, disconnect Surface Hub from any Wi-Fi networks (but keep Wi-Fi enabled), so you can control the channel used for Miracast. You can manually select the Miracast channel in Settings. You will need to restart Surface Hub after each change. Generally speaking, you will want to use channels that do not show heavy utilization from the network scan.

It is also possible that the connect issue can be the result of a problem on the connecting device. If the projecting device is running Windows, it should be Windows 8.1 or newer for full Miracast support. Again, for troubleshooting, disconnect the projecting device from any Wi-Fi networks. This will eliminate any channel switching between the access point channel and the Miracast channel set on Surface Hub. Also, some Group Policy and firewall settings may be tied to a Wi-Fi network.

It is also a good idea to ensure the latest drivers and updates are installed on the projecting device. In Device Manager, open the Wi-Fi adapter and video adapter and check for an updated driver version.

Next, ensure Miracast is supported on the device.

1. Press Windows Key + R and type dxdiag.
2. Click "Save all information".
3. Open the saved dxdiag.txt and find Miracast. It should say Available, with HDCP.

The Windows firewall can block Miracast traffic. The simplest test is to disable the firewall and test projection. If Miracast works with the firewall disabled, add an exception for:

C:\Windows\System32\WUDFHost.exe

Allow In/Out connections for TCP and UDP, Ports: All.

On domain-joined devices, Group Policy can also block Miracast.

Use the Windows Key + R and type `rsop.msc` to execute the Resultant Set of Policy snap-in. This will show the current policies applied to the PC.

Review Computer Configuration > Windows Settings > Security Settings > Wireless Network (IEEE 802.11) Policies. There should be a setting for wireless policies.

Double click the setting for wireless policies and a dialog box will appear.

Open the Network Permissions tab and select Allow everyone to create all user profiles.

The last place to check is in the Event logs. Miracast events will be logged to `Wlanautoconfig`. This is true on both Surface Hub and the projecting device. If you export Surface Hub logs, you can view Surface Hub's `Wlanautoconfig` in the `WindowsEventLog` folder. Errors in the event log can provide some additional details on where the connection fails.

### *Performance*

After wireless projection is connected, it is possible to see performance issues causing latency. This is generally a result of overall channel saturation or a situation that causes channel switching.

For channel saturation, refer to the network scan and try to use channels with less traffic.

Channel switching is caused when the Wi-Fi adapter needs to send traffic to multiple channels. Certain channels support Dynamic Frequency Selection (DFS). DFS is used on channels 49 through 148. Some Wi-Fi drivers will show poor performance when connected to a DFS channel. If you are seeing poor Miracast performance while connected to a DFS channel, try the projection on a non-DFS channel. Both Surface Hub and projecting device should use non-DFS channels.

If Surface Hub and the projecting device are both connected to Wi-Fi but using different access points with different channels, this will force Surface Hub and the projecting device to channel switch while Miracast is connected. This will result in both poor wireless projection and poor network performance over Wi-Fi. The channel switching will affect the performance of all wireless traffic, not just wireless projection.

Channel switching will also occur if the projecting device is connected to a Wi-Fi network using a different channel than the channel that Surface Hub uses for Miracast. So, a best practice is to set Surface Hub's Miracast channel to the same channel as the most commonly used access point.

If there are multiple Wi-Fi networks or access points in the environment, some channel switching is unavoidable. This is best addressed by ensuring all Wi-Fi drivers are up to date.

## Troubleshooting network and configuration issues

Surface Hub should always be connected to a wired network and requires DHCP for IP addressing. Make sure that Exchange services are available for email and calendar access on the device and Skype and/or Teams.

You can verify the device is connected to the internet by opening Edge to make sure the home page loads. Navigate to **Portal.Office.com** to make sure that you can log into Office 365 with your credentials as well as the resource account credentials for Surface Hub.

Open the Whiteboard and Export the image to bring up the Share pane. Select Email to make sure the device is able to send email from the resource account. You can also invite the resource account to a meeting and it should be displayed on the Welcome screen and Start menu.

Surface Hub requires the following open ports: 443 (HTTPS), 80 (HTTP), and 123 (NTP).

Additionally, there are ports required for Skype for Business depending on whether your Skype services are located in the cloud, on-premises, or hybrid.

For cloud ports see: [Office 365 ports](#)

For Skype on-premises see: [Skype On-premises ports](#)

### Proxy

If your organization restricts computers on your network from connecting to the Internet, there is a set of URLs that need to be available for devices to use Microsoft Store for Business. Some of the Store for Business features use Microsoft Store app and Microsoft Store services. Devices using Store for Business – either to acquire, install, or update apps – will need access to these URLs. If you use a proxy server to block traffic, your configuration needs to allow these URLs:

- login.live.com
- login.windows.net
- account.live.com
- clientconfig.passport.net
- windowsphone.com
- \*.wns.windows.com
- \*.microsoft.com
- www.msftncsi.com (prior to Windows 10, version 1607)
- www.msftconnecttest.com/connecttest.txt (replaces www.msftncsi.com starting with Windows 10, version 1607)



There are some errors that can come up when configuring Surface Hub with an account. If you experience issues during setup or assigning an account to the device review the following page for information on the error message.

<https://docs.microsoft.com/en-us/surface-hub/troubleshoot-surface-hub>

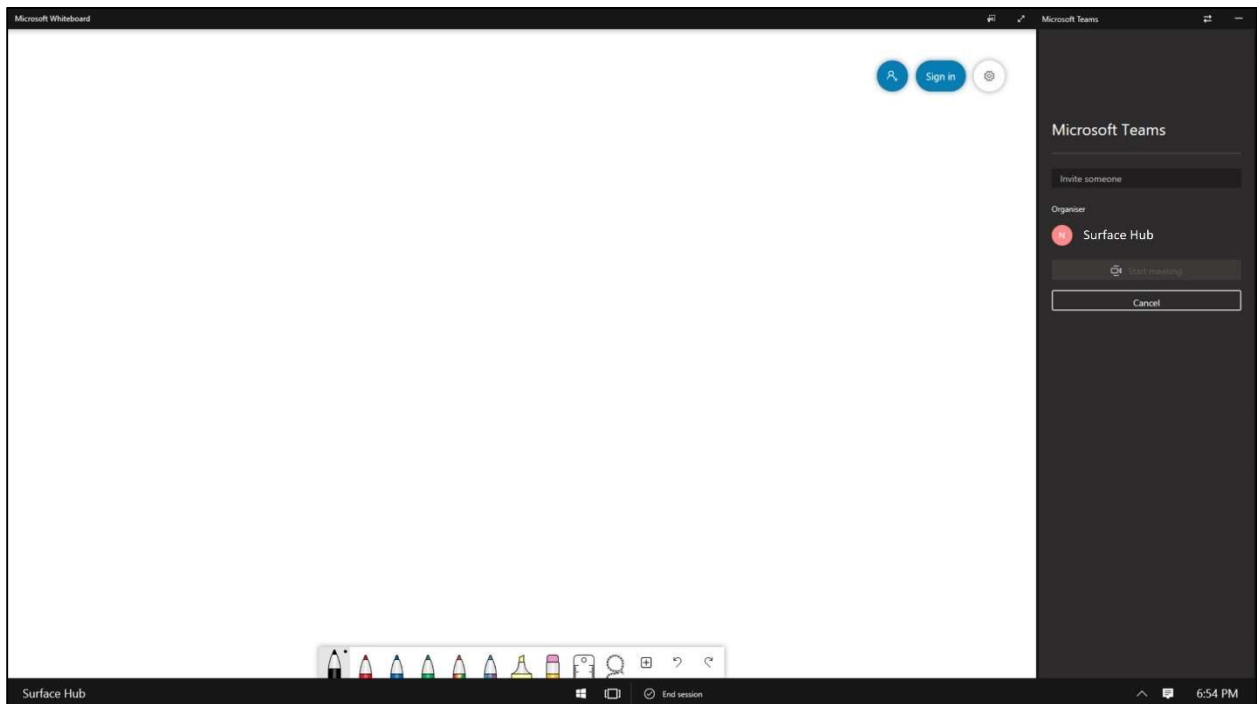
## Microsoft Teams and Skype for Business meetings

---

### Troubleshooting Microsoft Teams for meetings and presentations

Surface Hub is a Teams resource endpoint for meetings and presentations. As long as the account is configured properly and the Surface Hub can connect to Exchange with Active Sync, scheduled meetings will be displayed on the Welcome screen on the day of the meeting.

Surface Hub will sign into Teams as soon as the device is turned on and started up. To make sure that Teams is able to sign in, press the Call button on the Welcome screen.



You should see that Teams is ready to start a call by inviting someone to the meeting. If Teams can't sign in or doesn't start, try restarting the Surface Hub first to make sure it can connect and is using the latest applied settings.

The device account should also be able to sign into Teams using a web browser, so open Edge and navigate to [Teams.microsoft.com](https://teams.microsoft.com) and try to sign in with the account assigned to the device.

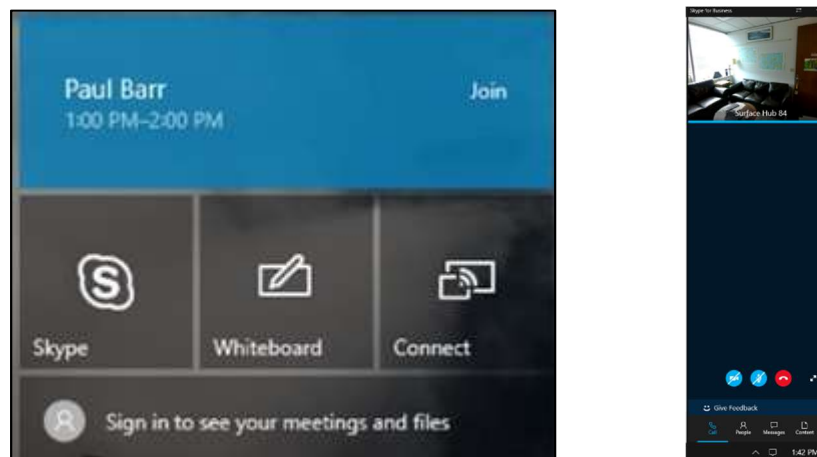
As a Teams admin, make sure that Teams is enabled for the account and that it is configured properly.

Users can join Teams meetings from any device with the Teams app, such as their mobile phone or laptop. Anyone you invite to a Teams meeting can join via a web browser for the basic meeting experience. You'll want to familiarize yourself with the various features of each app and understand the user experience.

## Troubleshooting Skype for Business for meetings and presentations

Surface Hub can also be used as a Skype for Business resource endpoint for Skype for Business meetings and presentations. As long as the account is configured properly and the Surface Hub can connect to Exchange with Active Sync, scheduled meetings will be displayed on the Welcome screen on the day of the meeting.

Depending on how your organization is rolling out or migrating from Skype for Business to Microsoft Teams, Surface Hub may have either Skype or Teams set as the default calling app. If Skype is the default calling app, then pressing the Skype button on the Welcome screen will start the Skype for Business application and allow users to make a call using Skype.



You can test the Skype account credentials by signing into Skype for Business on a PC, but it's not a fool-proof way to verify that the Surface Hub will work with Skype for Business, it just verifies that the credentials are correct. Surface Hub relies on Autodiscover to locate the Skype for Business server it should sign into. If your organization uses Skype for Business on-premises, and there is a certificate for authentication, Surface Hub will need to have that certificate manually added to its repository in settings.

Once the Surface Hub is signed into Skype for Business you should be able to join meetings and make calls from the device as expected. The user experience for Skype for Business is very similar between Surface Hub, PC, and mobile but you will want to be able to support users in meetings with any device.

You can troubleshoot most issues that occur during a meeting by leaving the meeting and rejoining the meeting, by pressing the red button and then Rejoin Meeting. If it's just a screen presentation issue, try pressing the Stop Presenting button and then Present Screen again.

## Let's Review

---

In this lesson, you learned:

- Users can collaborate in a wide variety of ways using Surface Hub and Microsoft Teams
- There are some simple troubleshooting steps to fix common issues that can arise during normal use
- How to assist users with Microsoft Teams and Skype for Business meetings

## 2. Surface Hub configuration best practices

---

### Lesson Objectives

---

After completing this lesson, you will be able to:

- Describe how resource accounts have been configured in your organization
- Monitor devices using Operations Management Suite
- Configure the device settings to best meet your user's needs

### Device Account configuration and provisioning

---

There are basic requirements for every organization that deploys Surface Hub. In this lesson you'll learn some best practices around resource account creation, deployment, and provisioning. Keep in mind that you may need to modify these steps to match your environment.

#### Resource account setup

The easiest way to configure a resource account for Surface Hub is to use a PowerShell script and run all of the commands as a global administrator. This is because there are requirements for Exchange, Skype, Office licensing, Teams, and Voice that require admin privileges.

Resource accounts can be created as new accounts or created from modified existing accounts. There are many scripts available online that can assist during the account creation process. Be sure to visit this site to familiarize yourself with the scripts and commands that are used to provision the account.

#### [PowerShell for Surface Hub](#)

Surface Hub requires the creation of a logon-enabled Exchange resource mailbox in Exchange 2013 or newer or Exchange Online which allows the device to maintain the meeting calendar, receive meeting requests and send email.

The mailbox needs to be configured with the correct properties to allow ease of scheduling. It also needs a compatible Mobile Device Mailbox policy where the PasswordEnabled property is set to False.

The account needs to have a license assigned and then enabled in Skype for Business and/or Teams in order to use conferencing features.

You may also need to whitelist the ActiveSync device ID of the Surface Hub if your organization has a global policy that prevents the device account from syncing the mail and calendar info.

Optionally, as a best practice consider turning off password expiration for the account and allow the Surface Hub to automatically rotate the password. If you need the password, for example during device troubleshooting, just reset the password via the administrator portal or PowerShell.

## Calendar processing best practices

Since the resource account for Surface Hub needs to be available for users to reserve on a first come first serve basis, you will want to ensure that certain calendar processing rules are configured properly.

For new users, one of the best ways to share information with them about the new technology that's available is to utilize the automatic response feature of the resource account.

```
Set-CalendarProcessing -Identity [device_account] -AddAdditionalResponse $true -AdditionalResponse "This is a Surface Hub room!"
```

The additional response can be customized with helpful information for users that can walk them through the basics of starting a meeting, connecting a device, and other tasks. You can use HTML code as well to format the message with bold text and bullet points in proper paragraphs as well.

It might be a good idea to put any organization specific information in the response email such as how to get in contact with support if they experience issues starting or during the meeting.

## Improve adoption with room lists

Teams takes advantage of Exchange's New-DistributionGroup cmdlet -RoomList switch. The RoomList switch specifies that all members of a specific distribution group are room mailboxes.

You can create as many distribution groups as you need – based on any parameter that you want. You may want to set up a list for rooms with a Surface Hub to make it easier for users to know which rooms have collaboration devices.

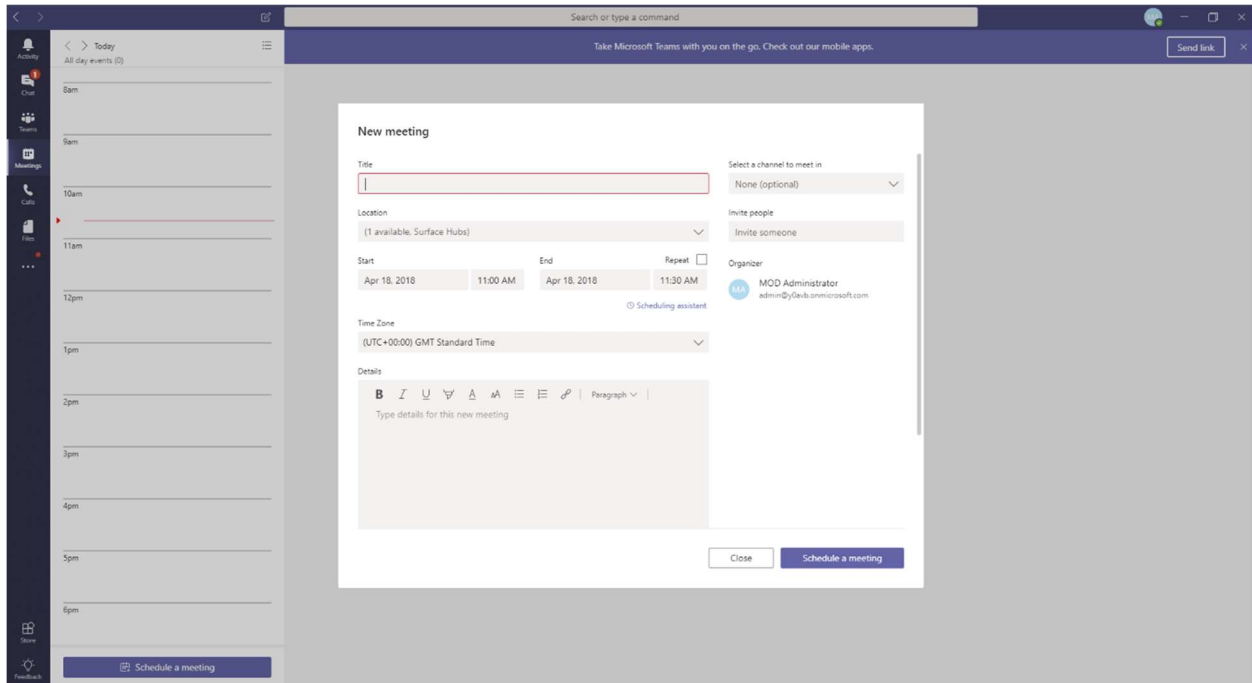
Create the new distribution groups with the -RoomList switch:

```
New-DistributionGroup -Name "Surface Hubs" -Roomlist
```

Add rooms to the distribution groups:

```
Add-DistributionGroupMember -Identity "Surface Hubs" -Member "SurfaceHub01"
```

Log back into your Teams client and see the new lists.



## Enable Voice calling in Teams and Skype

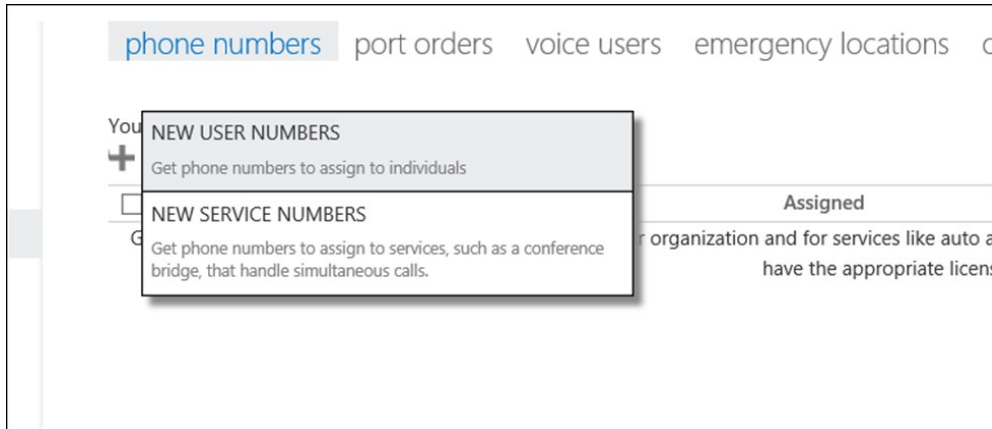
You can also allow your Surface Hub to make and receive public switched telephone network (PSTN) phone calls by enabling Enterprise Voice for your account. Making and receiving phone calls with Office 365 requires a Dial Plan license, either Domestic or Domestic and International.

Enterprise Voice isn't a requirement for Surface Hub, but if you want PSTN dialing functionality for the Surface Hub client, here's how to enable it:

On-premises configuration requires a domain controller, and a phone number-

```
Set-CsMeetingRoom -Identity HUB01 -DomainController DC-ND-001.contoso.com -LineURI "tel:+14255550555;ext=50555" -EnterpriseVoiceEnabled $true
```

Office 365 configuration be done in the Skype for Business legacy portal-

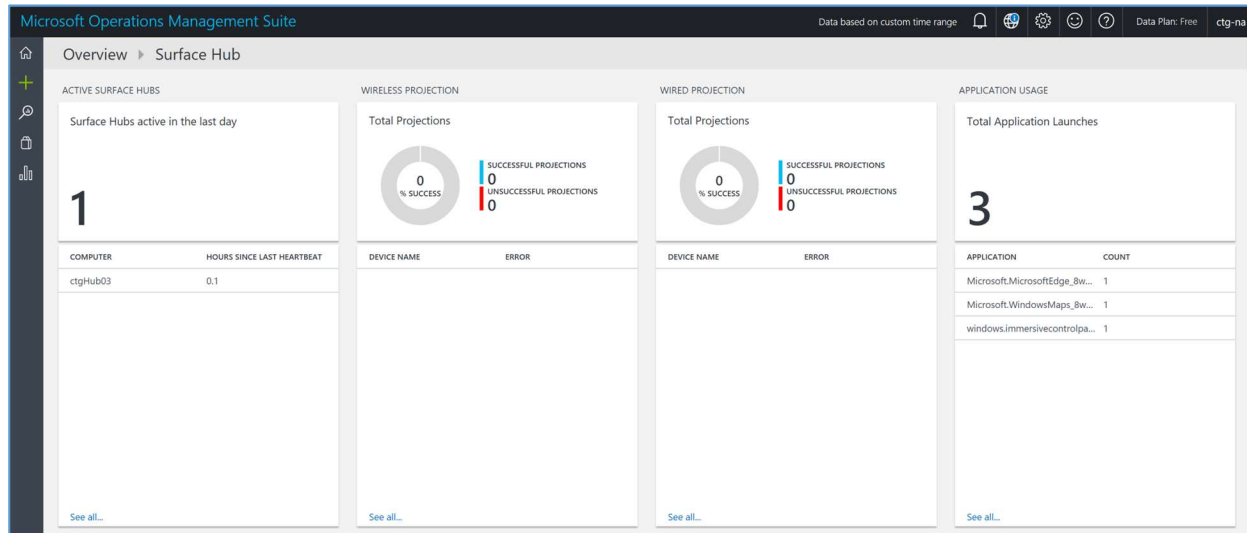


After acquiring a phone number, with a Dial Plan license assigned to the Surface Hub device account, assign the number to the account to enable the Surface Hub to make and receive PSTN phone calls.



## Monitor device with Operations Management Suite

Microsoft Operations Management Suite (OMS) is an IT management solution that helps you manage and protect your entire IT infrastructure, including your Surface Hubs. Surface Hub is offered as a custom-built Log Analytics solution in OMS, allowing you to collect and view usage and reliability information across all Surface Hubs in your organization.



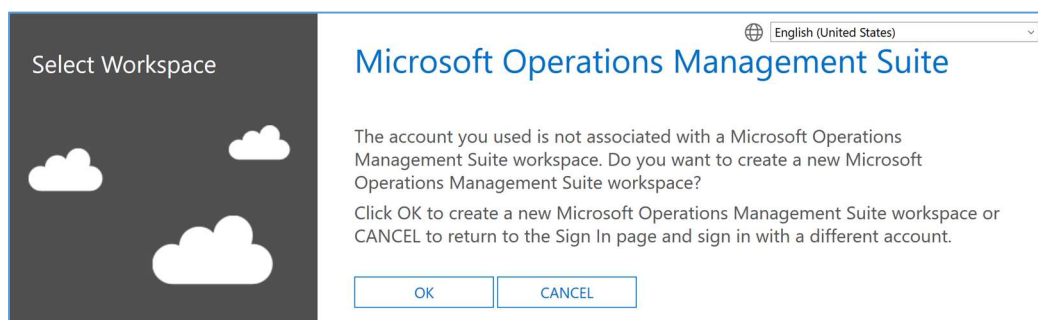
### Setup and configure Operations Management Suite

One of the first things you'll need to do is set up an Azure subscription if your organization doesn't have one already.

You can access Azure by logging to your organization's Office 365 Admin portal at **portal.office.com** or by navigating to **portal.azure.com** and signing in with admin credentials for your organization.

Operations Management Suite (OMS) is a web-based portal that uses workspaces to view and manage your data. You can access OMS by browsing to **mms.microsoft.com** and signing in with either a Microsoft Account or a Work or School account. If your organization is using Azure Active Directory (Azure AD), use a Work or School account to sign in.

Once you are signed in, you'll have the option to create a new OMS workspace.

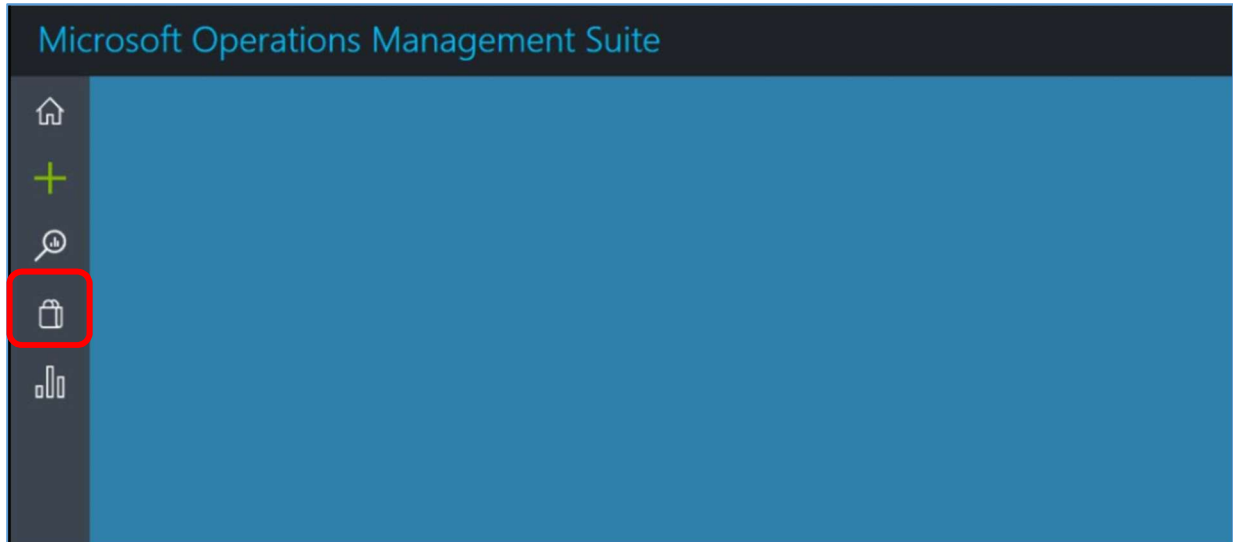


## Microsoft Surface Hub 2S

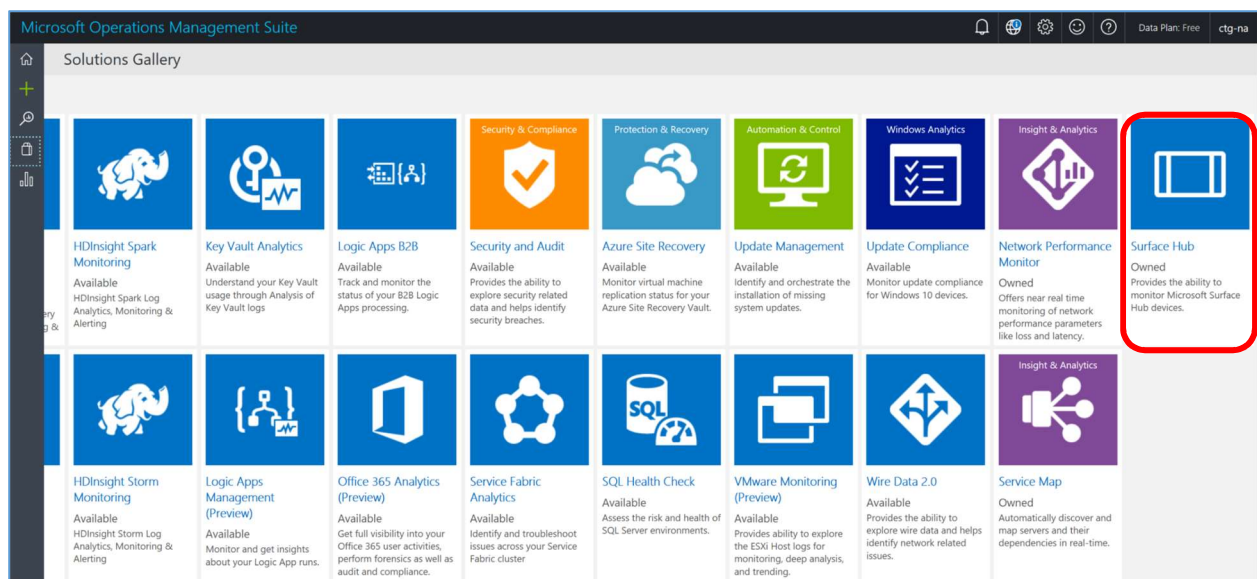
Click OK to create a new OMS workspace.

After you create the workspace, you will need to link the new OMS workspace to an Azure subscription for your organization. If you don't have an Azure subscription, you can create a new subscription at this point. In order to use an existing subscription, you will need an Azure administrator to grant access to the subscription.

The Microsoft Operations Management Suite portal will open to a new dashboard view. On the left side of the screen is a menu of icons. Select the **Solutions Gallery** icon (shopping bag) to open the gallery.



In the Solutions Gallery, scroll to the right and click the **Surface Hub** tile.



## Monitor the health and status of devices

Now that you have Operations Management Suite set up and ready to go, you need to enroll your Surface Hubs so that they start sending their telemetry data to your workspace. There are several ways to enroll Surface Hubs in OMS, which we will walk through in detail here. You can choose the method that makes the most sense for your organization.

First, you will need to locate your OMS Workspace ID and Key. These are the codes that you will need to enter on your Surface Hubs to enroll them with your OMS.

In the OMS portal, navigate to the **Settings**.

Then select **Connected Sources** from the list on the left.

The Windows Servers sources will be selected by default. On the right, you will see the Workspace ID along with Primary and Secondary Key codes. You will need the Workspace ID and the Primary Key to enroll your Surface Hubs. There are several methods for enrolling Surface Hubs and some may be easier than others depending on your organization's setup. For now, just remember that this is where we can find the right keys.

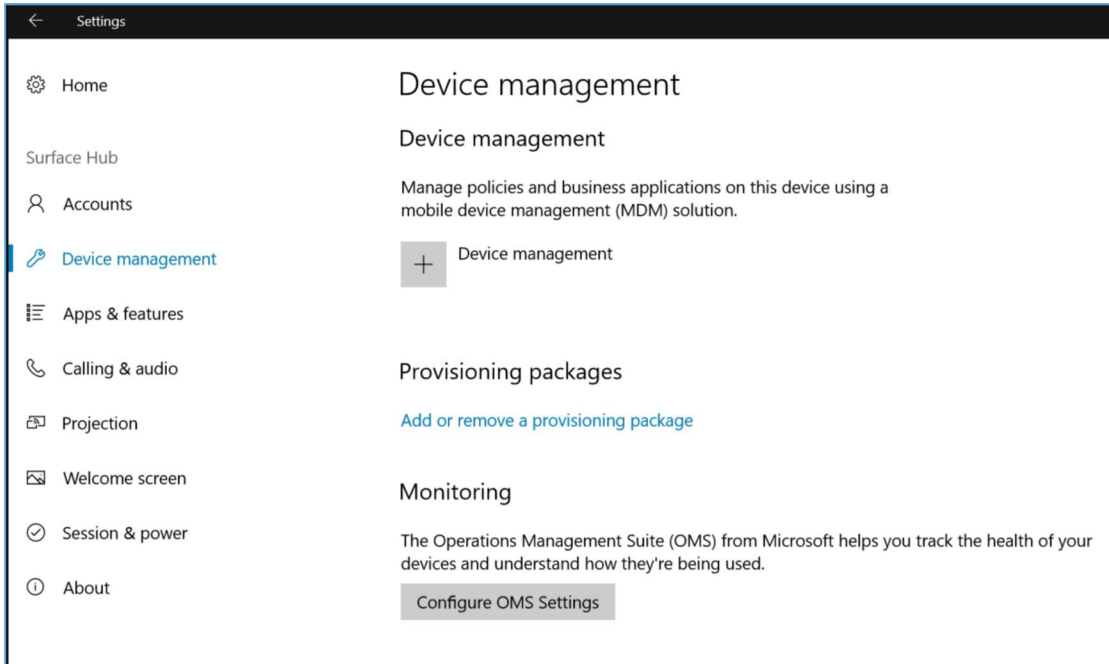
For Surface Hub to connect and register with the OMS service, it must have access to specific sites on certain ports. Surface Hub **DOES NOT** currently support the use of a proxy server to communicate with the OMS service.

<u>Agent resource</u>	<u>Ports</u>	<u>Bypass HTTPS inspection?</u>
*.ods.opinsights.azure.com	443	Yes
*.oms.opinsights.azure.com	443	Yes
*.blob.core.windows.net	443	Yes
ods.systemcenteradvisor.com	443	No

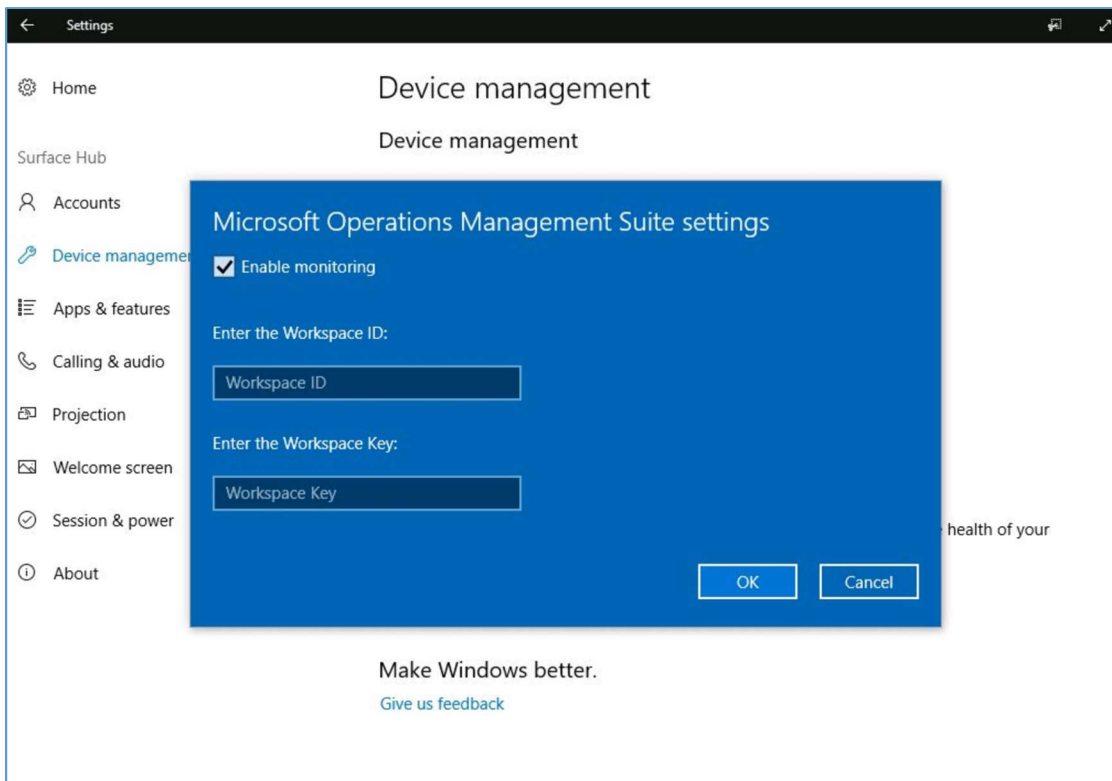
The Microsoft Monitoring Agent, used to connect devices to OMS, is integrated into the Surface Hub operating system (Windows 10 Team Edition), so there is no need to install additional clients to connect Surface Hub to OMS.

You can enroll a Surface Hub into OMS using the Local Settings on the device. This process requires administrator access on the Surface Hub so make sure you are authorized to access the Settings on your Surface Hub. At the Surface Hub screen, open **Start > All Apps > Settings**.

Then choose **Surface Hub > Device management** to access the Monitoring option for Surface Hub.



Click **Configure OMS Settings** to bring up the settings dialog box.

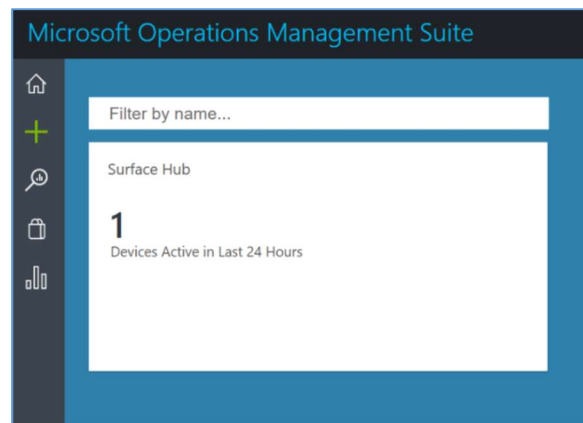


Check the box for **Enable monitoring**. Then type in the **Workspace ID** and **Workspace Key** (Primary) that you located in the OMS Settings in the portal. When you are finished, click **OK**.

There are several ways to make this process easier since both the ID and Key are complex character strings.

1. Access the OMS Portal using the Edge browser on Surface Hub, open **mms.microsoft.com** and sign in with your credentials. Then access the OMS settings in the portal and copy and paste the ID and Key into the OMS settings on the Surface Hub.
2. Establish an ad-hoc Skype for Business call between your PC and the Surface Hub, then copy and paste the ID and Key into the Conversation window in the call. This enables you to access the ID and key from the Messages panel on the Surface Hub and copy and paste the ID and Key into the respective boxes in settings.
3. Create a document that contains the Workspace ID and Key and save that document to OneDrive or USB flash drive. Open the document on the Surface Hub and copy and paste the ID and Key into the respective boxes in settings.

Once you have successfully enrolled the Surface Hub with OMS, it will start to send data to the service. You should start seeing telemetry data for your Surface Hub in the OMS Portal after a short period of time.



The Surface Hub OMS dashboard is a great tool for monitoring your Surface Hubs. You can get use the available queries to get a quick sense of how your Surface Hubs are operating and which features your users are using the most. Proactive management and issue resolution will help you stay ahead of any problems your users may be experiencing.

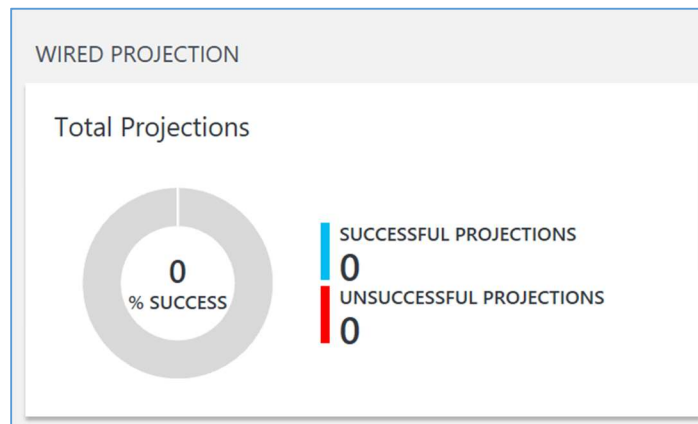
From the Overview page in your OMS workspace, click the **Surface Hub** tile to view the Surface Hub dashboard. You can change the time range for the whole dashboard at the top of the screen.

The Active Surface Hubs view is used to get an inventory of all your Surface Hubs. Once connected to OMS, each Surface Hub periodically sends a "heartbeat" event to the service. This view shows Surface Hubs that have reported a heartbeat in the last 24 hours by default.

The Wireless Projection view is used to get usage and reliability data for wireless projection over the past 24 hours by default but you can change the time range. The graph shows the total number of wireless connections across all your Surface Hubs, which provides an indication of whether users in your organization are using this feature. If it is a low number, it may suggest a need to provide additional training. You can use the filters to show the number for a specific Surface Hub.

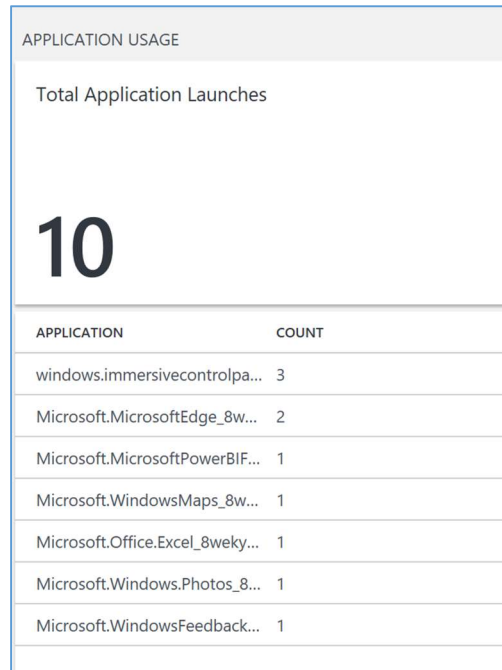
The graph on the dashboard overview shows a breakdown of successful and unsuccessful connections. If there are a high number of unsuccessful connections, devices may not properly support wireless projection using Miracast.

The Wired Projection view shows successful and unsuccessful wired projections to the Surface Hub.



Click the view to see more detailed information on the wired connections that have been recorded in OMS. If this graph shows a high number of unsuccessful wired connections, it may indicate a connectivity issue in your audio-visual pipeline. For example, if you use a HDMI repeater or a center-of-room control panel, it may need to be restarted.

The Application Usage view is a great tool to see what apps your users are using in their meetings and collaboration sessions. This records an event each time an app is launched, not including Skype for Business, on a Surface Hub in your organization.



APPLICATION USAGE

Total Application Launches

**10**

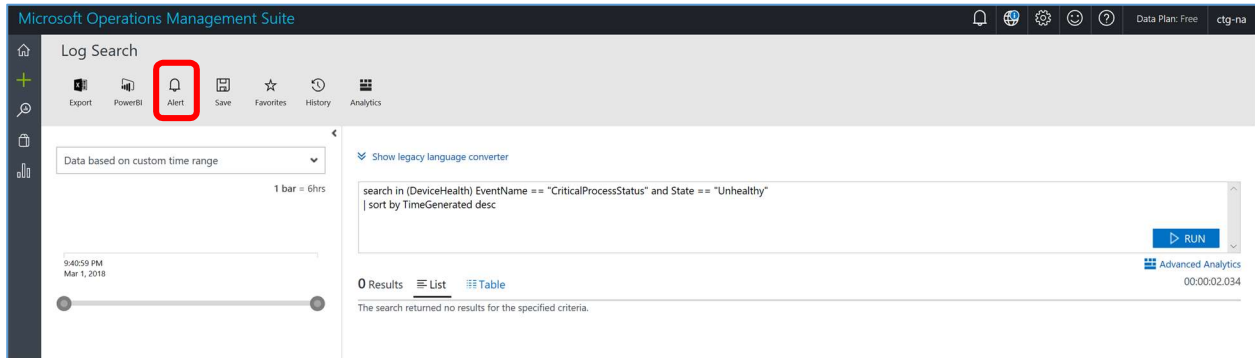
APPLICATION	COUNT
windows.immersivecontrolpa...	3
Microsoft.MicrosoftEdge_8w...	2
Microsoft.MicrosoftPowerBIF...	1
Microsoft.WindowsMaps_8w...	1
Microsoft.Office.Excel_8weky...	1
Microsoft.Windows.Photos_8...	1
Microsoft.WindowsFeedback...	1

Using this tool, you can start to get an idea of what users are doing in their meetings, and by opening the detailed view, you can filter the events by Surface Hub. Some Surface Hubs may be seeing a higher utilization of certain apps more than others. For example, Surface Hubs in lounge areas may see a higher use of the Whiteboard while Surface Hubs in traditional conference rooms may see a higher use of PowerPoint.

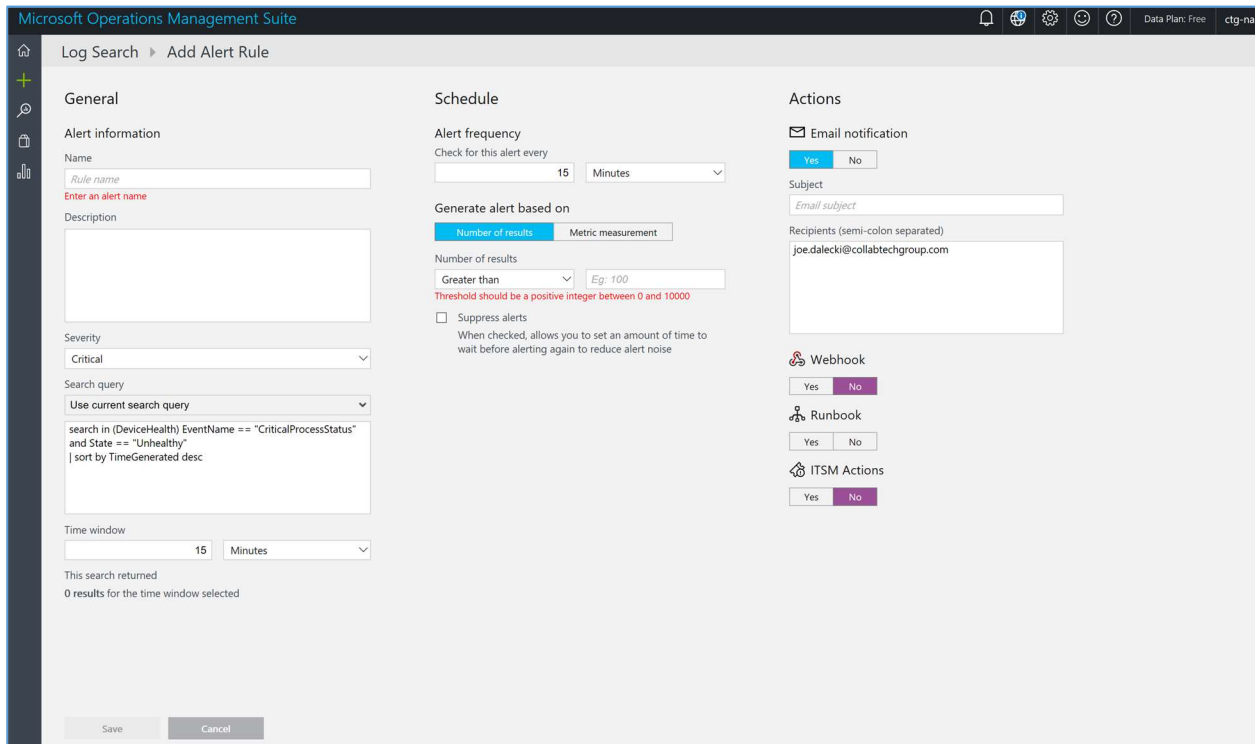
A helpful tool for detecting poorly behaving in-box apps and evaluating new line-of-business apps on your Surface Hubs is the Application Crashes view in the Surface Hub dashboard.

## Use alerts to receive pro-active notifications

To set up a custom alert and receive a notification when specified criteria are met use the dashboard to view a saved or sample query.



In the Log Search view, select **Alert**.



On the Add Alert Rule page, enter a **name** for the Alert rule, which will help you identify the alert in OMS. Enter a brief **description** of the Alert that might include the logic behind the use of the alert. Select the **severity** of the alert from Critical, Warning, or Informational. A critical warning would be an alert that requires immediate attention while an informational alert would be something you just want to keep track of.



You can see the search query that is going to be run in the box, in our example we are monitoring for suggested device reboot events.

The Time window specifies the time range for the query. The query only returns event records that were created within this range of time. It can be set from 5 minutes to 25 hours and needs to be set wide enough to account for reasonable delays in event reporting. Generally, the Time window should be set to twice the longest expected delay so that alerts are not missed.

For more information on setting a Time window, refer to: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-alerts>.

Next, you need to set the schedule for the query to run. The Frequency specifies how often the query should run, which can be set from 5 minutes to 24 hours, and should be less than or equal to the Time window so that alerts are not missed.

The Threshold allows you to set criteria for alert creation as a number of results or metric measurement. If you select a number of results threshold, a single alert is created when the number of records returned by the log search query exceed the specified number. If you select a metric measurement threshold, an alert is created for each object in the results of the log search query with values that exceed the specified threshold.

To avoid multiple redundant alerts from being created, you can use Suppress Alerts to suppress alerts for at least as long as the Time window.

For more information on Frequency and Threshold settings, refer to: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-alerts>.

Finally, you need to specify an action that will be performed when the alert is created. The most common action is to send an email notification for the alert. By specifying the subject of the email notification, you could use Outlook conditional formatting or handling rules to automate processing. You can also add multiple recipients in the Recipients box by separating each one with a semi-colon.

Additionally, you could configure a Webhook to invoke an external process through a single HTTP POST request, or a Runbook to start a runbook in Azure Automation. More information on both of these types of actions can be found at: <https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-alerts-actions>.

When you are finished setting up the Alert Rule, click **Save**. The alert will now monitor your Surface Hub logs and notify you if errors are found.

## Walkthrough device settings and best practices

---

### Installing and removing apps for users

Surface Hub runs Windows 10 Team Edition, which means that only Store apps that are enabled for Surface Hub can be installed on the device. End users can not access and download apps from the Store onto the device. Only administrators can access the Settings and open the Store to install apps.

As an admin, open settings, and go to Surface Hub, then Apps & features.

On the page, select the button to Open Store.

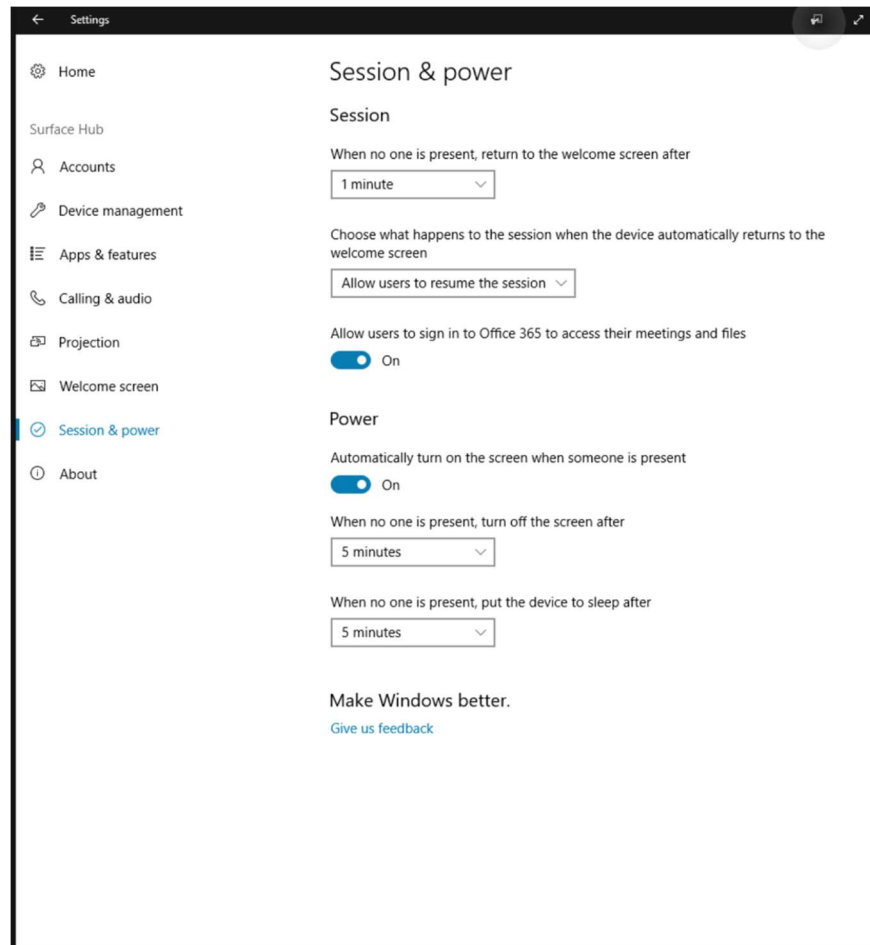
In the store, search for or browse to the app that you want to install. If it is not listed in the Store on a Surface Hub, then it is not available for that device.

When you select Install on an app, it may ask you to sign in with a Microsoft Account. This is optional and allows you to add apps to your account for other devices.

To remove an app that has been installed on Surface Hub, on the Apps & features page of settings, scroll down through the list to locate the app you want to remove and select Uninstall. Some apps cannot be uninstalled this way as they are built into the core operating system image.

### Changing sleep and session settings based on room type

Depending on the use of the space and/or the use of the device, you may want to consider modifying the default values for screen, sleep, and session time out settings.



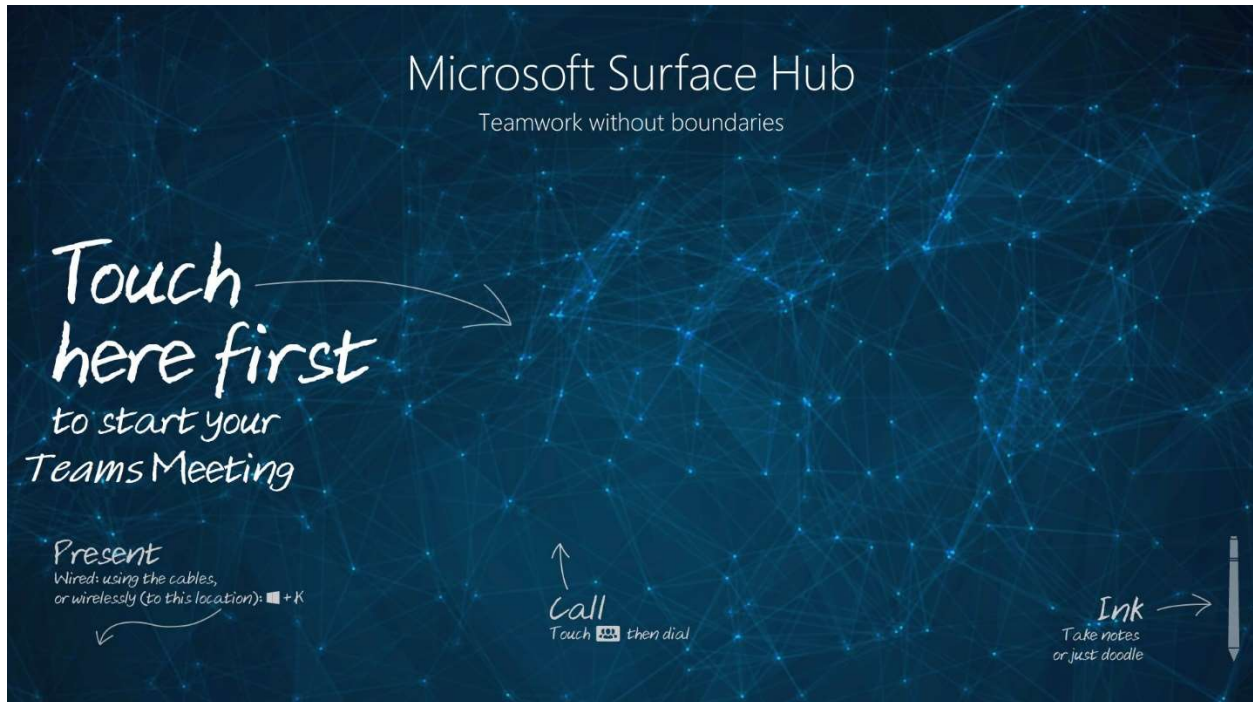
For example:

A space that is not normally reservable and is used primarily for brief ad-hoc standup meetings – Surface Hub should be set to time out after only a brief time (1-2 minutes) and possibly automatically end the session instead of allowing the session to be resumed. This keeps the security risk of unintentionally exposing sensitive information to a minimum without interrupting a typical meeting.

A space that is only booked through exchange and used for long periods of time by the same group for project meetings or training seminars – Surface Hub should be set to time out after a long time of inactivity (1-2 hours) and possibly allow resuming of a suspended session. This allows more flexibility in the use of the space but puts more responsibility on the users to ensure they are protecting sensitive information by signing out or using End Session.

## Configure a branded Welcome screen and custom Start menu tiles

You can upload and set a custom background wallpaper in the Settings on Surface Hub. The wallpaper you use could be branded with your company logo or other important information for users such as where to touch the screen to join their meeting. Consider something like the following example:



The resolution of the screen is 3840 x 2560 (3:2) so you will want to select a background image that matches that resolution and is not stretched.

The January 17, 2018 update to Windows 10 (build 15063.877) enables customized Start menus on Surface Hub devices. You apply the customized Start menu layout using mobile device management (MDM).

When you apply a customized Start menu layout to Surface Hub, users cannot pin, unpin, or uninstall apps from Start.

The customized Start menu is defined in a Start layout XML file. You have two options for creating your Start layout XML file:

Edit the default Surface Hub Start XML or configure the desired Start menu on a desktop (pinning only apps that are available on Surface Hub), and then export the layout.

There are a few key differences between Start menu customization for Surface Hub and a Windows 10 desktop:

- You cannot use DesktopApplicationTile (<https://docs.microsoft.com/windows/configuration/start-layout-xml->

- desktop#startdesktopapplicationtile) in your Start layout XML because Windows desktop applications (Win32) are not supported on Surface Hub.
- You cannot use the Start layout XML to configure the taskbar or the Welcome screen for Surface Hub.
  - Surface Hub supports a maximum of 6 columns (6 1x1 tiles), however, you must define GroupCellWidth=8 even though Surface Hub will only display tiles in columns 0-5, not columns 6 and 7.
  - Surface Hub supports a maximum 6 rows (6 1x1 tiles)
  - SecondaryTile, which is used for links, will open the link in Microsoft Edge.

For example XML files and more information, check out <https://docs.microsoft.com/en-us/surface-hub/surface-hub-start-menu>

## Let's Review

---

In this lesson, you learned how to:

- Describe how resource accounts have been configured in your organization
- Monitor devices using Operations Management Suite
- Configure the device settings to best meet your user's needs

## 3. Manage Surface Hub updates and recovery

---

### Lesson Objectives

---

After completing this lesson, you will be able to:

- Setup and configure Surface Hub for Intune
- Manage Windows updates and app updates to all devices
- Initiate device recovery and re-configuration

### Setup and configure Surface Hub for Intune

---

#### Configure Intune to manage Surface Hub

Surface Hub and other Windows 10 devices allow IT administrators to manage settings and policies using a mobile device management (MDM) provider. A built-in management component communicates with the management server, so there is no need to install additional clients on the device.

Surface Hub has been validated with Microsoft's first-party MDM providers:

- On-premises MDM with System Center Configuration Manager (beginning in version 1602)
- Hybrid MDM with System Center Configuration Manager and Microsoft Intune
- Microsoft Intune standalone

You can also manage Surface Hubs using any third-party MDM provider that can communicate with Windows 10 using the MDM protocol.

To configure manual enrollment

1. On your Surface Hub, open Settings.
2. Type the device admin credentials when prompted.
3. Select Surface Hub and navigate to Device management.
4. Under Device management, select + Device management.
5. Follow the instructions in the dialog to connect to your MDM provider.

You can use MDM to manage some Surface Hub CSP settings, and some Windows 10 settings. Depending on the MDM provider that you use, you may set these settings using a built-in user interface, or by deploying custom SyncML. Microsoft Intune and System Center Configuration Manager provide built-in experiences to help create policy templates for Surface Hub. Refer to documentation from your MDM provider to learn how to create and deploy SyncML.

You can use Microsoft Intune to manage Surface Hub settings. For Platform, select Windows 10 and later, and in Profile type, select Device restrictions (Windows 10 Team).

Microsoft Intune includes many built-in settings to control different features on a device. You can also create custom profiles. Custom profiles are great when you want to use device settings and features that aren't built in to Intune. These profiles include features and settings for you to control on devices in your organization.

Windows 10 custom profiles use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure different features. These settings are typically used by mobile device manufacturers to control features on the device.

For more information on creating custom profiles in Intune refer to: <https://docs.microsoft.com/en-us/intune/custom-settings-windows-10>.

### Push configuration profiles to groups of devices

To make managing devices easier, you can use Microsoft Intune device categories to automatically add devices to groups based on categories that you define.

You can create any device categories you want. For example:

- Point-of-sale device
- Demonstration device
- Sales
- Accounting
- Manager

For more information on creating Intune groups refer to: <https://docs.microsoft.com/en-us/intune/device-group-mapping>.

Common Windows 10 Team settings can be found here: <https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10-teams>.

### Push Store apps to devices

The Microsoft Store for Business gives you a place to find and purchase apps for your organization, individually, or in volume. By connecting the store to Microsoft Intune, you can manage volume-purchased apps from the Azure portal. For example:

- You can synchronize the list of apps you have purchased (or that are free) from the store with Intune.



- Apps that are synchronized appear in the Intune administration console; you can assign these apps like any other apps.
- You can track how many licenses are available, and how many are being used in the Intune administration console.
- Intune blocks assignment and installation of apps if there are an insufficient number of licenses available.
- Apps managed by Microsoft Store for Business will automatically revoke licenses when a user leaves the enterprise, or when the administrator removes the user and the user devices.

Review the following information before you start syncing and assigning apps from the Microsoft Store for Business:

- Configure Intune as the mobile device management authority for your organization.
- You must have signed up for an account on the Microsoft Store for Business.
- Once you have associated a Microsoft Business Store account with Intune, you cannot change to a different account in the future.
- Apps purchased from the store cannot be manually added to or deleted from Intune. They can only be synchronized with the Microsoft Store for Business.
- Both online and offline licensed apps that you have purchased from the Microsoft Store for Business are synced into the Intune portal. You can then deploy these apps to device groups or user groups.
- Online app installations are managed by the store.
- Offline apps that are free of charge can also be synced to Intune. These apps are installed by Intune, not by the store.
- To use this capability, devices must be joined to Active Directory Domain Services, or workplace-joined.
- Enrolled devices must be using the 1511 release of Windows 10 or later.

Additionally, related sets and Offline Licensed apps synced from the Microsoft Store for Business will now be consolidated into a single app entry in the UI. Any deployment details from the individual packages will be migrated over to the single entry. To view related sets in the Azure portal, select App licenses from the Client apps blade.

Before you enable synchronization in the Intune console, you must configure your store account to use Intune as a management tool:

- Ensure that you sign into the Microsoft Store for Business using the same tenant account you use to sign into Intune.
- In the Business Store, choose the Manage tab, select Settings, and choose the Distribute tab.
- If you don't specifically have Microsoft Intune available as a mobile device management tool, choose Add management tool to add Microsoft Intune. If you don't have Microsoft Intune activated as your mobile device management tool, click Activate next to Microsoft

Intune. Note that you should activate Microsoft Intune rather than Microsoft Intune Enrollment.

The next step is to configure synchronization.

1. Sign into the Azure portal.
2. Choose All services > Intune. Intune is located in the Monitoring + Management section.
3. On the Intune pane, choose Client apps.
4. On the Client apps pane, choose Setup > Microsoft Store for Business.
5. Click Enable.
6. If you haven't already done so, click the link to sign up for the Microsoft Store for Business and associate your account as detailed previously.
7. From the Language drop-down list, choose the language in which apps from the Microsoft Store for Business are displayed in the Azure portal. Regardless of the language in which they are displayed, they are installed in the end user's language when available.
8. Click Sync to get the apps you've purchased from the Microsoft Store into Intune.

Then synchronize the apps. In the Client apps workload, choose Setup > Microsoft Store for Business. Click Sync to get the apps you've purchased from the Microsoft Store into Intune.

To assign an app to a group in Intune:

1. Sign in to the Azure portal.
2. Select All services > Intune. Intune is located in the Monitoring + Management section.
3. In the Intune menu, select Client apps.
4. In the Manage section of the menu, select Apps.
5. In the Apps pane, select the app you want to assign.
6. In the Manage section of the menu, select Assignments.
7. Select Add Group to open the Add group pane that is related to the app.
8. For the specific app, select an assignment type:
  - Available for enrolled devices: Assign the app to groups of users who can install the app from the Company Portal app or website.
  - Available with or without enrollment: Assign this app to groups of users whose devices are not enrolled with Intune. Users must be assigned an Intune license, see Intune Licenses.
  - Required: The app is installed on devices in the selected groups. Some platforms may have additional prompts for the end user to acknowledge before app installation begins.
  - Uninstall: The app is uninstalled from devices in the selected groups if Intune has previously installed the application onto the device via an "Available for enrolled devices" or "Required" assignment using the same deployment. Web links cannot be removed after deployment.

9. To select the groups of users that are affected by this app assignment, select **Included Groups**.
10. After you have selected one or more groups to include, select **Select**.
11. In the **Assign** pane, select **OK** to complete the included groups selection.
12. If you want to exclude any groups of users from being affected by this app assignment, select **Exclude Groups**.
13. If you have chosen to exclude any groups, in **Select groups**, select **Select**.
14. In the **Add group** pane, select **OK**.
15. In the app **Assignments** pane, select **Save**.

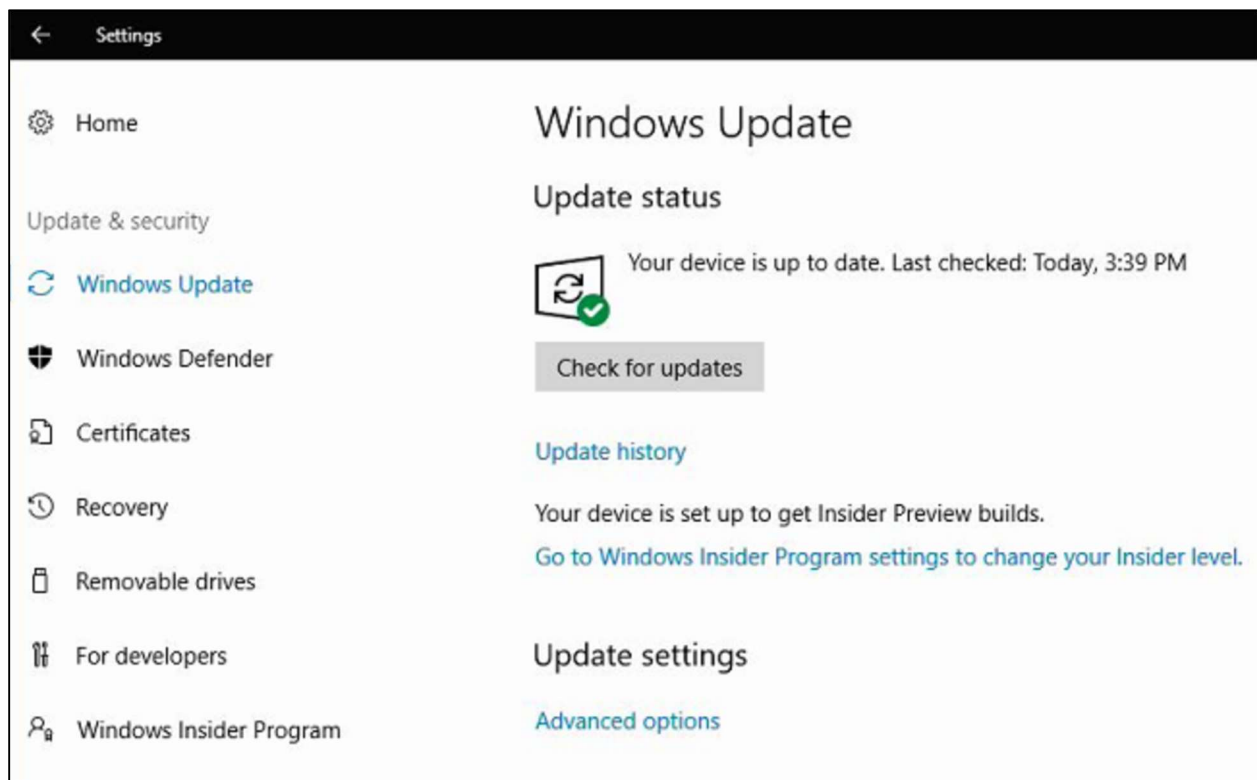
## Manage Windows Updates

### Managing auto updates for Windows 10 Team

Since Windows 10 Team Edition is designed to only work on Surface Hub, it has a few apps and features embedded into it that would require special attention when new features are released to Windows 10.

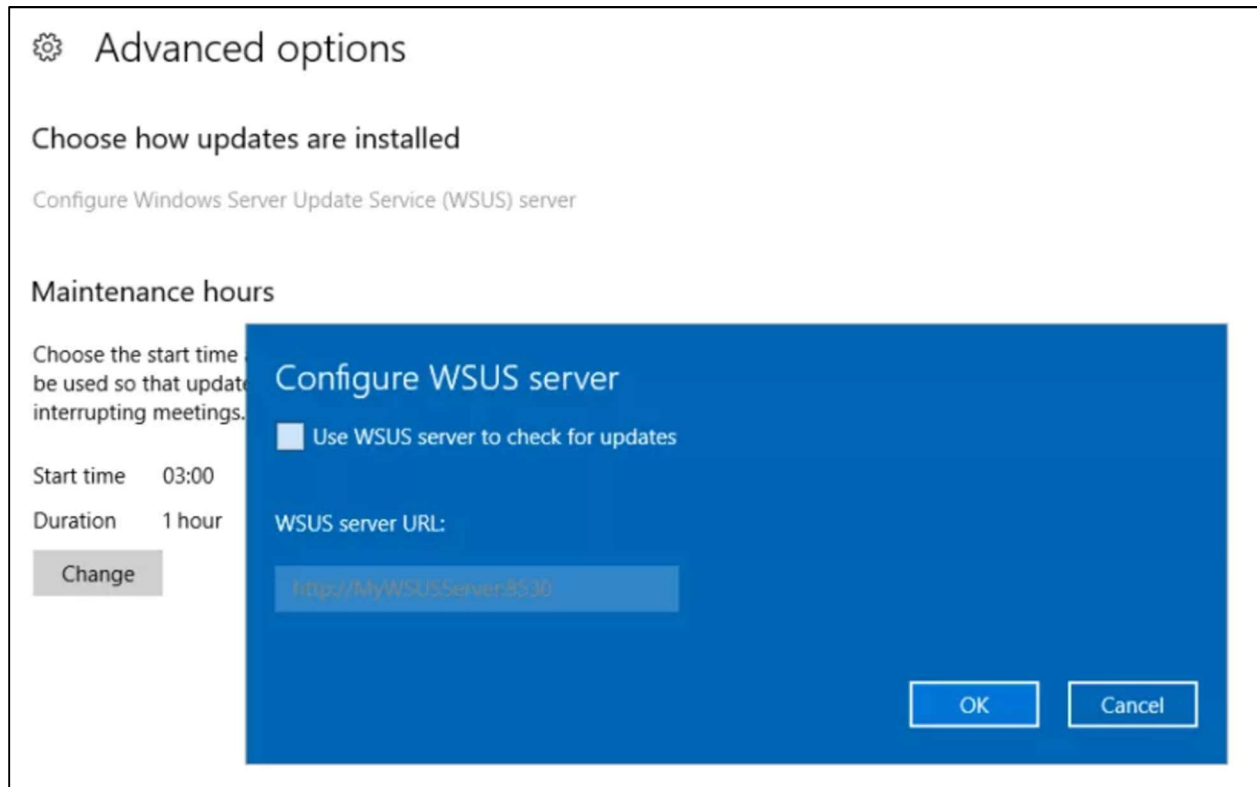
Windows 10 Team on Surface Hub is designed to be managed with automatic updates applied during a configurable nightly maintenance window or with Windows Server Update Services in your environment. You should enable updates for Surface Hubs you have deployed in your organization to ensure that they are running the latest versions of the operating system including Windows Defender for threat detection.

As an admin, open Settings, and select Update & Security.



On the Windows Update page, you can manually Check for updates by pressing the button or set the Update settings by selecting Advanced options.

The advanced options allow you to specify a WSUS server to use for updates and the start time and duration of the maintenance window.



If your organization uses a WSUS server for updates, enter the server URL in the settings.

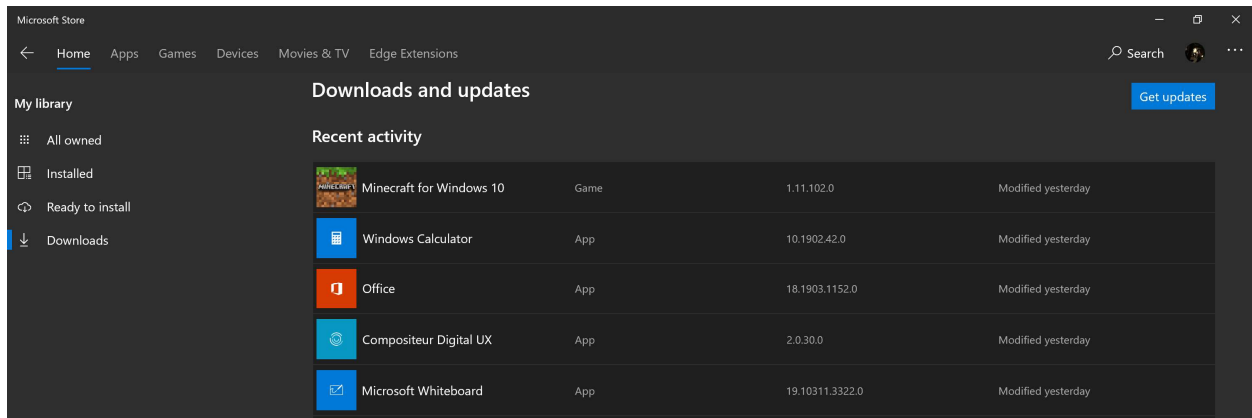
The default maintenance hours start at 3:00am local time and last for 1 hour. This means that if the Surface Hub is in use or scheduled to be in use for any time between 3:00am and 4:00am the nightly maintenance will be deferred to the next available window. One hour is usually enough time for most updates to be installed, however there are cases where a large release could take more than the allotted time, and if that happens be aware that the updates could still be in progress after the maintenance window has passed.

If a Surface Hub device has been turned off or disconnected from the internet for a long period of time (more than a few weeks) updates may automatically be installed when the device is turned on or connected to the internet again (regardless of maintenance hours). Make sure that you plan ahead if you are moving devices or leaving them off for a while, that you check for updates when you put them back into production.

## Update apps in the Store

During the nightly maintenance window, Surface Hub will check the Store for app updates and install any updates that are available for all installed apps on the device. You can also manually check for updates in the Store by opening the Store via Settings > Apps & features and selecting the ... menu in the top right corner, then Downloads and Updates.

If an app is experiencing issues or not performing as expected, try checking for app updates in the Store.



You can also try to uninstall problem apps and then reinstall apps. It is recommended that during troubleshooting you only install one app at a time and then test each app as they are installed to make sure there are no conflicts or unexpected behavior exhibited by any of the apps you have installed.

Windows Store for Business allows you to download app package files and install them on Surface Hub via Provisioning package or Intune. Apps installed this way must be updated by installing the updated app package file.

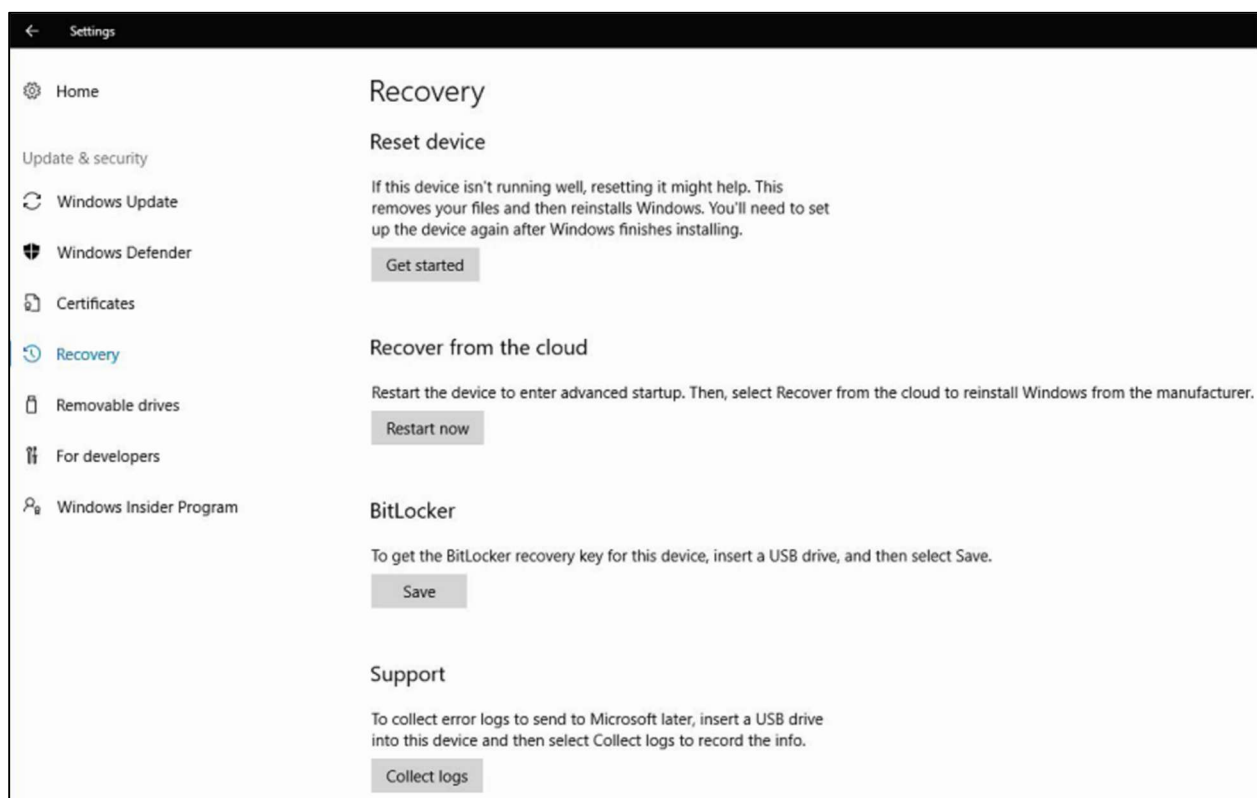
## Device Recovery and Re-configuration

### Using Settings to factory restore Surface Hub

There are two ways to recover the OS image on Surface Hub – a factory reset and a cloud download recovery.

Both of these can be initiated in the Settings, under Update & security.

A reset will restore the OS to the Out-Of-Box-Experience and allow you to reconfigure the device. This can take anywhere from 1-2 hours typically so it should not be performed unless all other troubleshooting steps have been taken first.



Select Get started to begin the Reset process.

The option to Recover from the cloud will use a downloaded image from Microsoft to attempt to restore the operating system image. Selecting Restart now will reboot the Surface Hub to the advanced startup options and allow a cloud recovery to begin.

It is highly recommended that you first make sure you have the BitLocker key for the device before you attempt a cloud recovery in case you are asked to enter it in the advance startup menu.

Insert a USB drive into the device and select Save to write a text file to the device with the 48 character BitLocker key to it.

Microsoft Surface Hub 2S

### [Downloading a recovery image](#)

[Waiting on information on Bare Metal Reset recovery tool for the 128GB M.2 NVMe drive]



## Let's Review

---

In this lesson, you learned how to:

- Setup and configure Surface Hub for Intune
- Manage Windows updates and app updates to all devices
- Initiate device recovery and re-configuration