Surface Hub documentation

Surface Hub 2S is an all-in-one digital interactive whiteboard, meetings platform, and collaborative computing device.

What's new

HOW-TO GUIDE

Microsoft Teams Rooms on Windows comes to Surface Hub 2S

New Teams Rooms licensing requirements

Change display language on Surface Hub

Surface Hub & Teams Rooms automated setup guide (requires M365 authentication)

Install Windows 10 Team 2022 Update

Install Progressive Web Apps on Surface Hub

Install & manage Surface Hub 2 Smart Camera

Teams Rooms on Surface Hub

Troubleshoot

HOW-TO GUIDE

Troubleshoot Teams sign-in issues on Surface Hub

Troubleshoot Surface Hub 2S Power Issues

Troubleshoot access to Settings app on Surface Hub

Troubleshoot Surface Hub 2 pen

Troubleshoot display projection on Surface Hub

Recover & reset Surface Hub 2S

Recover Surface Hub v1 from the cloud

Collect Surface Hub log files

Surface Hub Update History

Service & support

REFERENCE

Get support

Surface Hub support solutions

Service & warranty

Surface Hub warranty & protection plans

Surface Hub driver & firmware support lifecycle

Get started

TRAINING

Prepare your environment for Surface Hub

Surface Hub 2S adoption and training guides

Surface Hub 2S adoption videos

Surface Hub 2S adoption welcome screens

Setup & deploy

DEPLOY

Surface Hub & Teams Rooms setup best practices

Set up Coordinated Meetings with Teams Rooms & Surface Hub

Surface Hub 2S adoption & training

Create & test a device account

See Surface Hub in action

VIDEO

Microsoft Mechanics Surface Hub playlist

The new Surface Hub 2 Smart Camera

Meetings & collaboration for hybrid teams

Beneath the Surface | Surface Hub & the hybrid workplace

New hybrid meeting experiences & manageability options

Enabling inclusive hybrid meetings with Microsoft Teams & Teams devices

REI embraces hybrid work & supporting sustainability goals with Surface Hub

Manage

GET STARTED

Manage Microsoft Teams settings on Surface Hub

Manage Surface Hub with an MDM provider

Manage local settings

Secure

GET STARTED

Surface Hub security overview

Configure passwordless sign-in on Surface Hub

Secure & manage Surface Hub 2S with SEMM & UEFI

Design, develop, & distribute

TRAINING

Design basics for Windows apps

Get started building Windows apps that work on all Windows devices

Test Surface Hub apps using Visual Studio

Distribute LOB apps to enterprises

Microsoft Store for Business

Distribute apps with a management tool

Community

TRAINING

Join the Surface Hub Technical Community

Install Windows 10 Team 2022 Update

Article • 02/02/2023 • Applies to: Surface Hub, Surface Hub 2S

An updated version of the Surface Hub operating system, **Windows 10 Team 2022 Update**, based on Windows 10 version 22H2, is now becoming available for Surface Hub 2S and the original Surface Hub (v1).

Distribution

You can obtain the 2022 Update for Windows 10 Team using one of the following methods:

- **Windows Update for Business**. Available starting on October 19, 2022 but governed by WUfB policy configuration.
- **Windows Update.** Availability will be phased by country/region, as noted in the following table:

Phase	Country/Region	Starting
1	Canada, New Zealand, Belgium	Late October
2	United Kingdom, Japan, Switzerland, Italy	Early November
3	United States, Germany	Mid November
4	Global	Late November

Servicing Surface Hubs with Windows 10 Team Edition version 20H2

Full servicing support for Windows 10 Team Edition version 20H2 is scheduled to continue until May 9, 2023. Be sure to update your devices to the 22H2-based version before this date to continue receiving Windows Updates.

2S devices

Customers can update their Surface Hub 2S devices to the 2022 Update through Windows Update, or Windows Update for Business. An updated bare metal recovery (BMR) image for use with the Hub 2S USB recovery process is not available at this time.

V1 devices

Customers can update their Surface Hub v1 devices to the 2022 Update through Windows Update, or Windows Update for Business. The Surface Hub Recovery Tool can also be used to re-image a device with the 2022 Update.

Learn more

- Surface Hub Update History

First time setup for Surface Hub

Article • 04/05/2023 • Applies to: Surface Hub, Surface Hub 2S

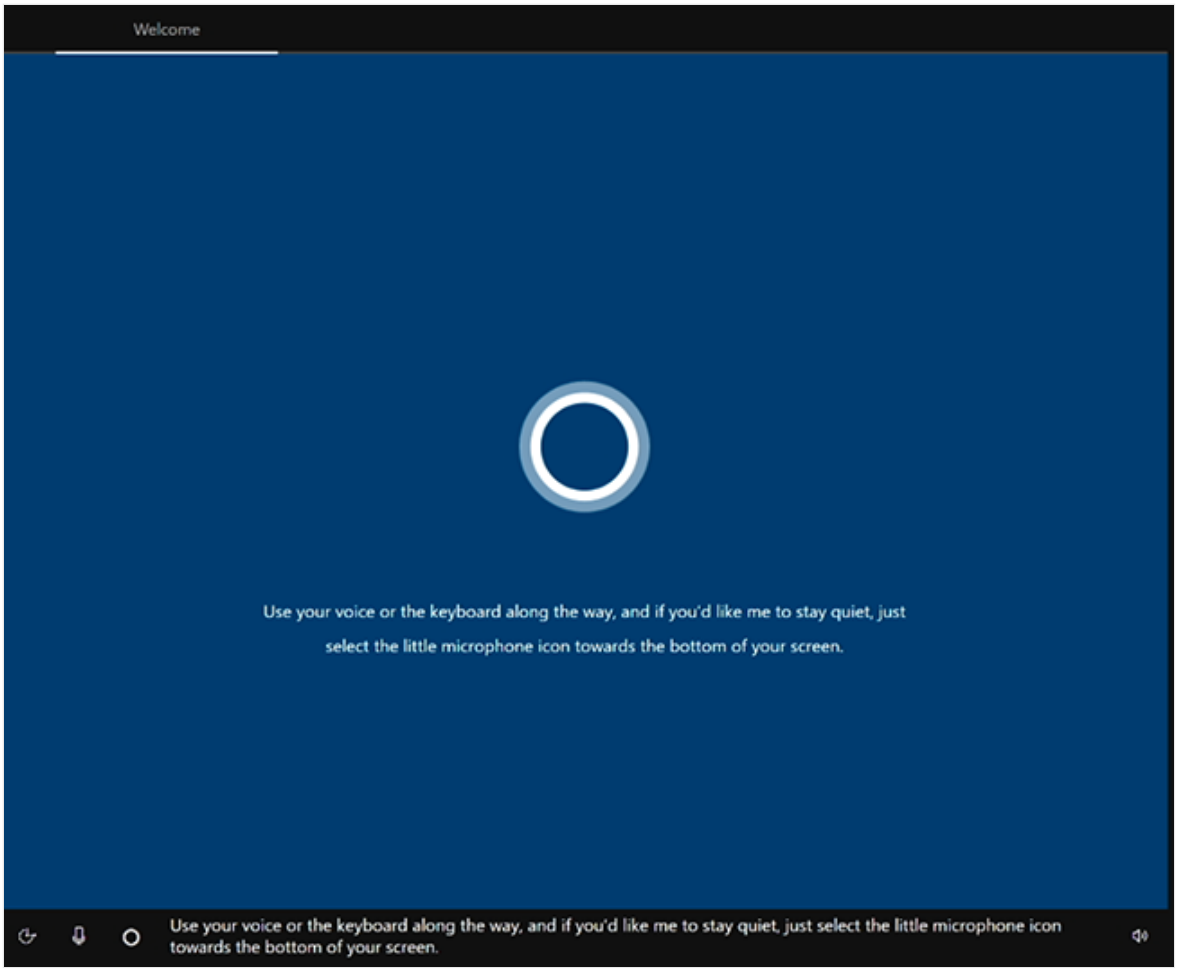
When you first start Surface Hub, the device automatically enters first time Setup mode to guide you through account configuration and related settings.

> **Tip**
>
> As a companion to this article, we recommend using the **Surface Hub and Microsoft Teams Rooms automated setup guide** when signed in to the Microsoft 365 Admin Center. This guide will customize your experience based on your environment. If you're hosted in Exchange Online and using Microsoft Teams, the guide will automatically create your device account with the correct settings. Or use it to validate existing resource accounts to help turn them into compatible Surface Hub device accounts. To review best practices without signing in and activating automated setup features, go to the **M365 Setup portal**.

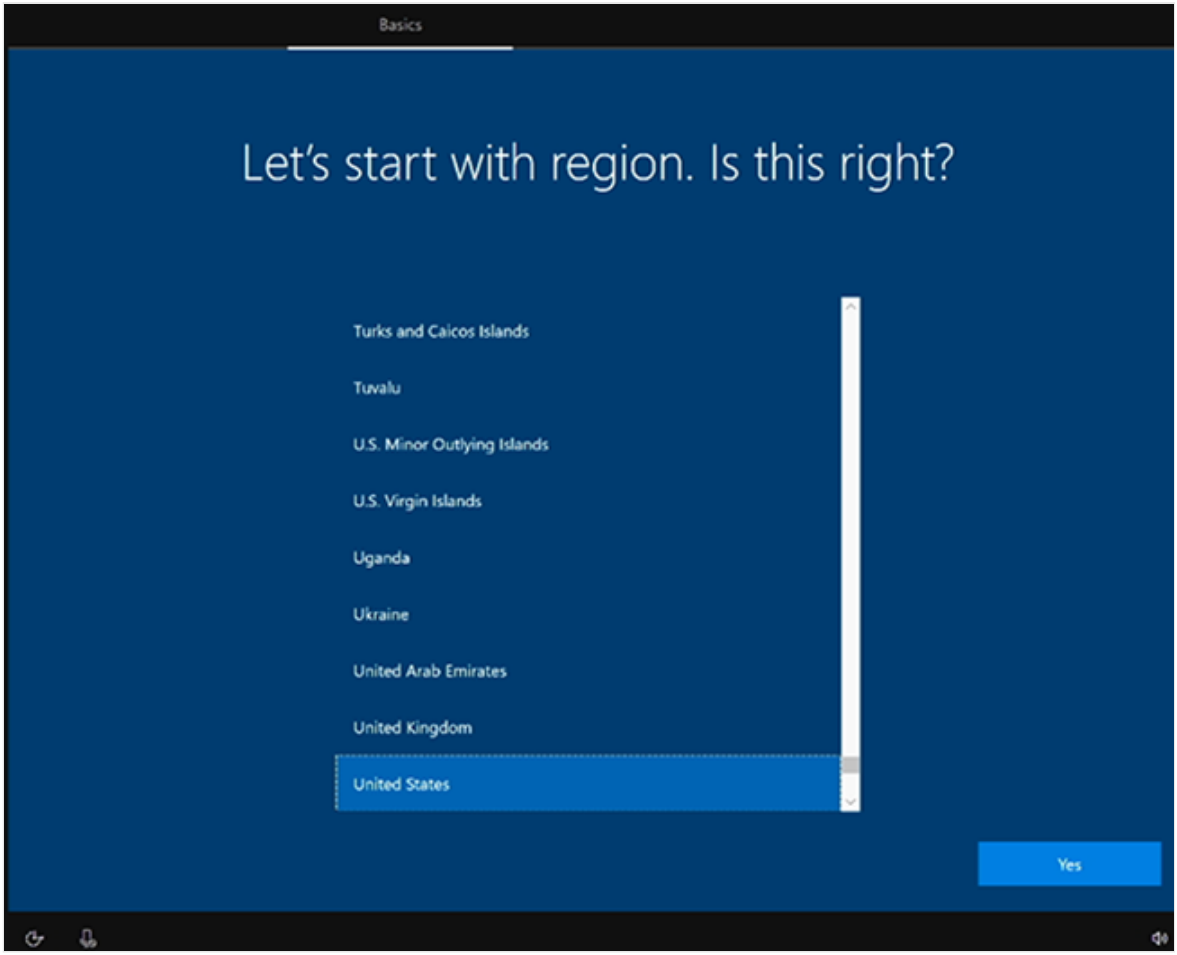
> **Note**
>
> You can automate the entire setup process with a **Provisioning package** to ensure a consistent experience across multiple Surface Hubs.

Get started

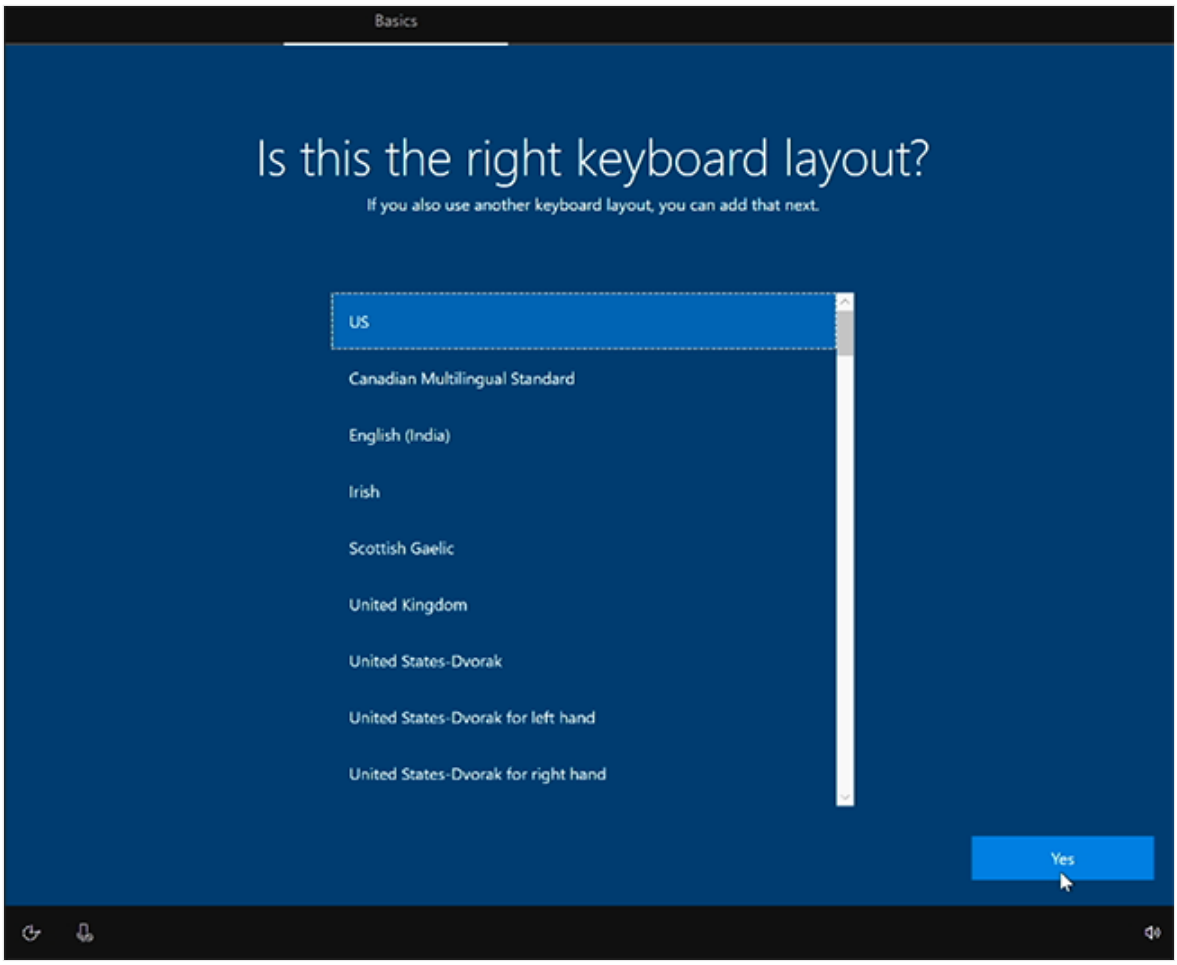
1. By default, Cortana is enabled to guide you through the process. To turn off Cortana assistance, select the microphone icon.



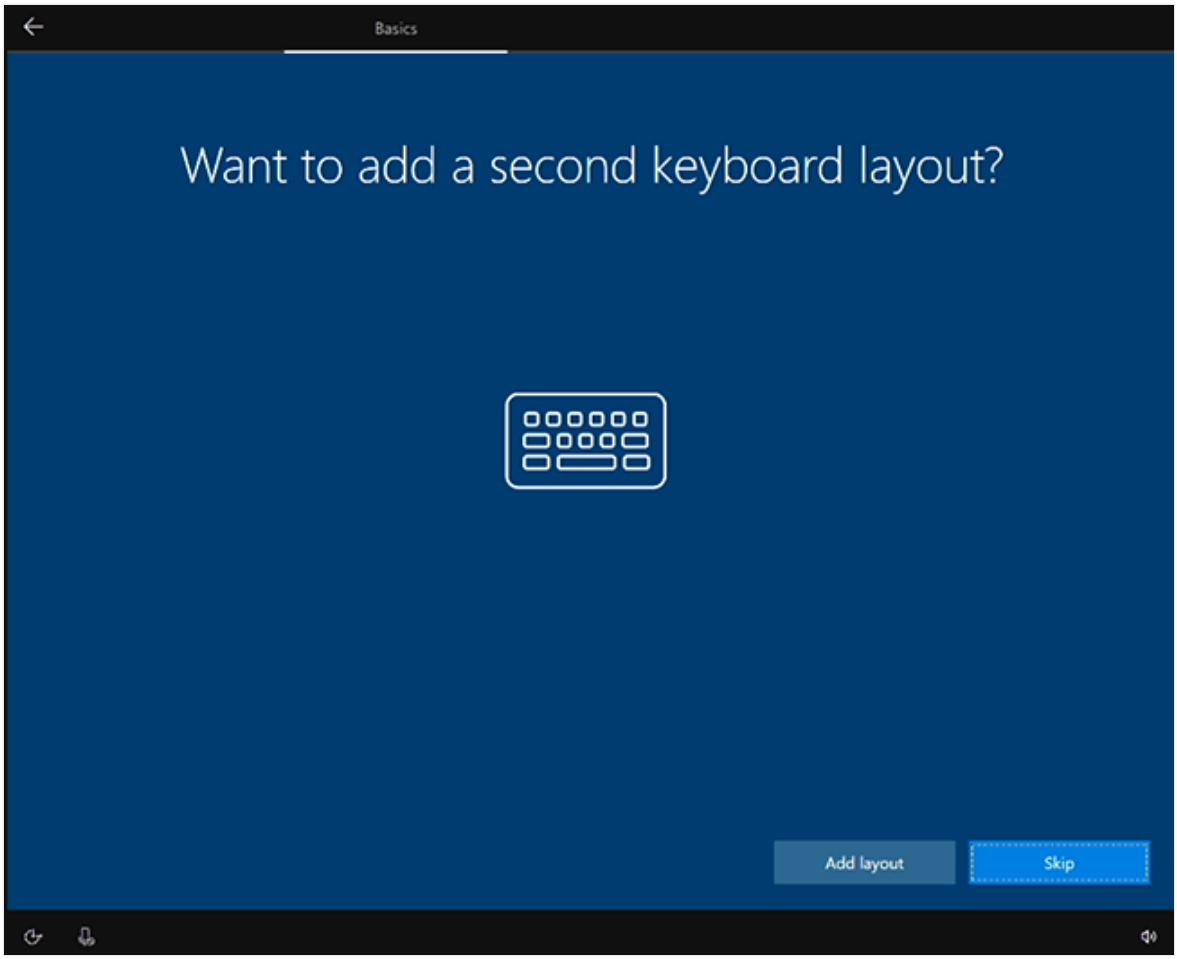
2. **Select your region.** Confirm the auto-detected region and select **Yes**.



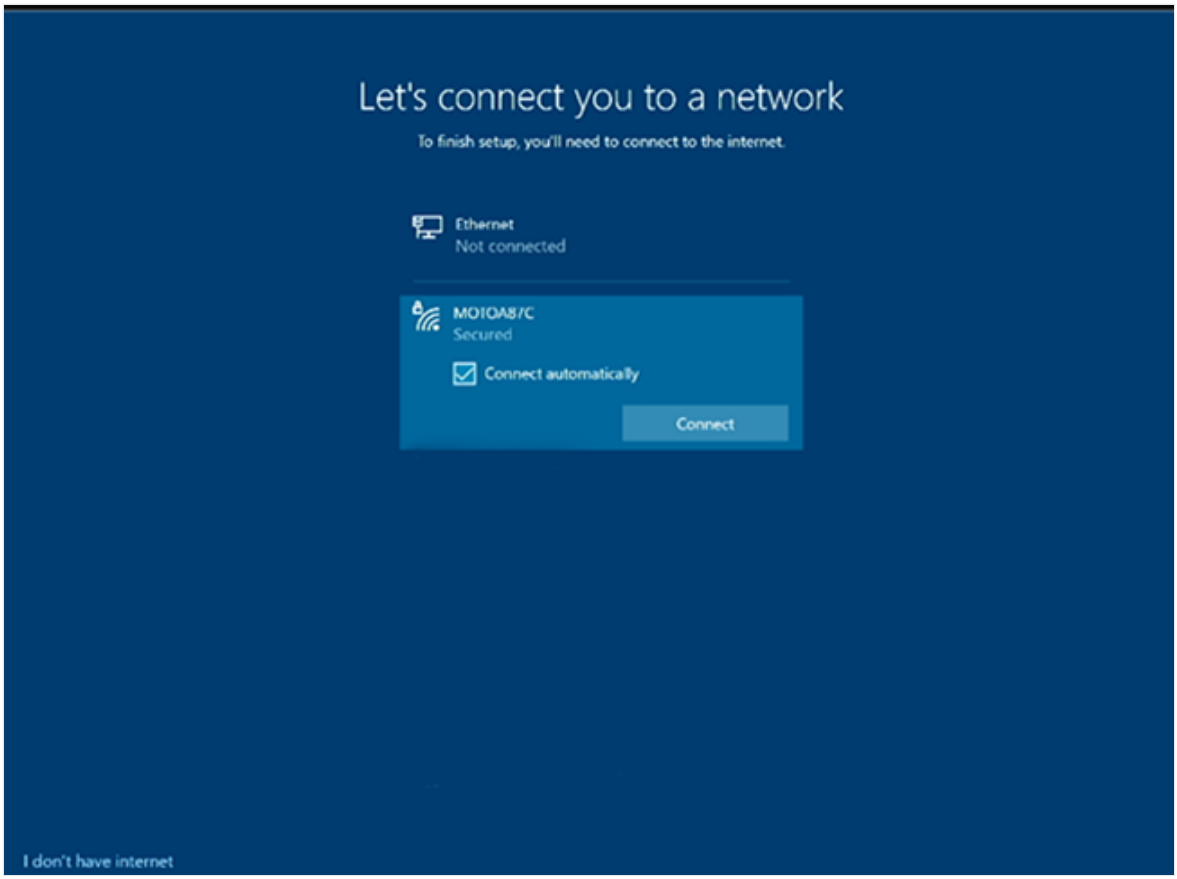
3. **Confirm keyboard layout.** Select **Yes**.



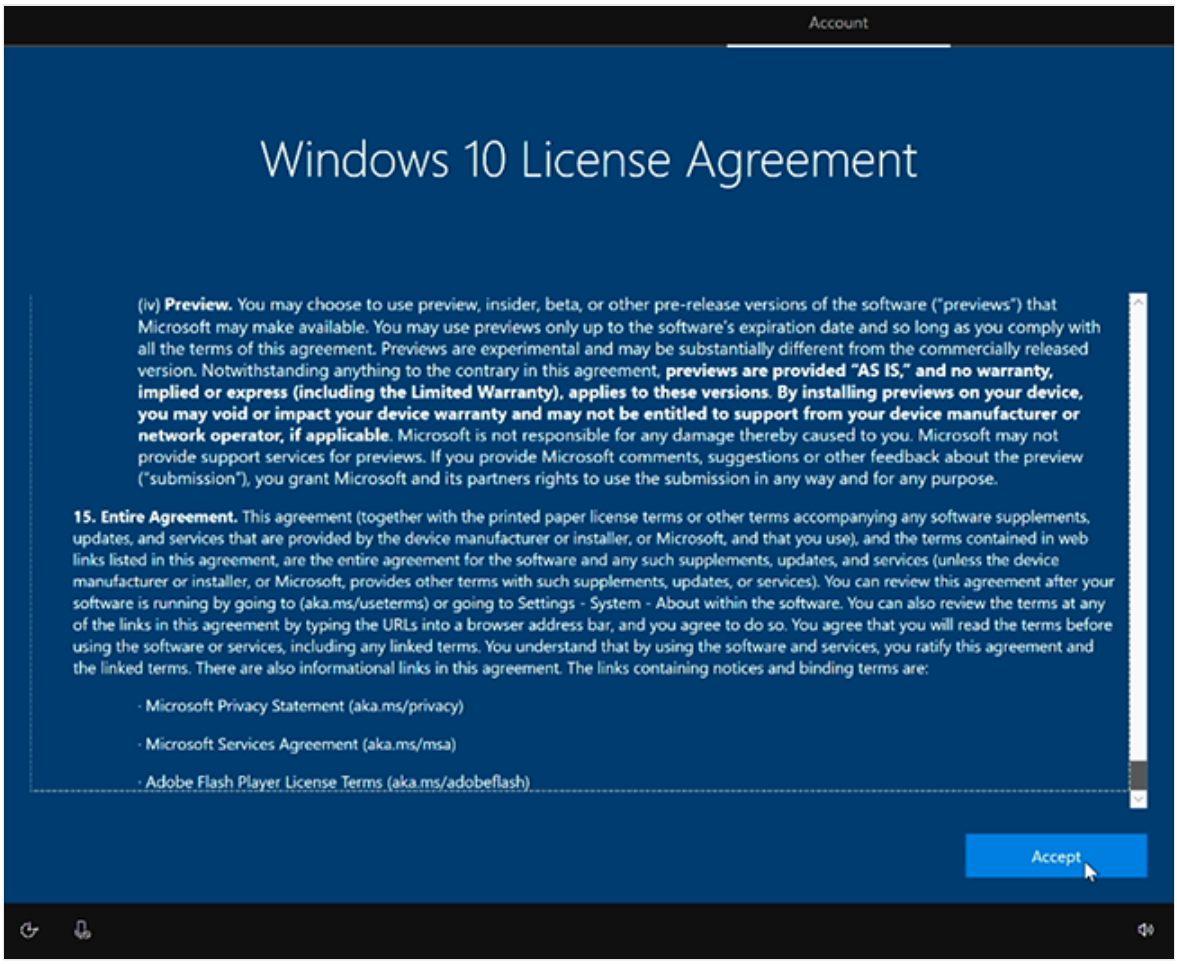
4. To add a second keyboard, select **Add layout**. Otherwise, select **Skip**.



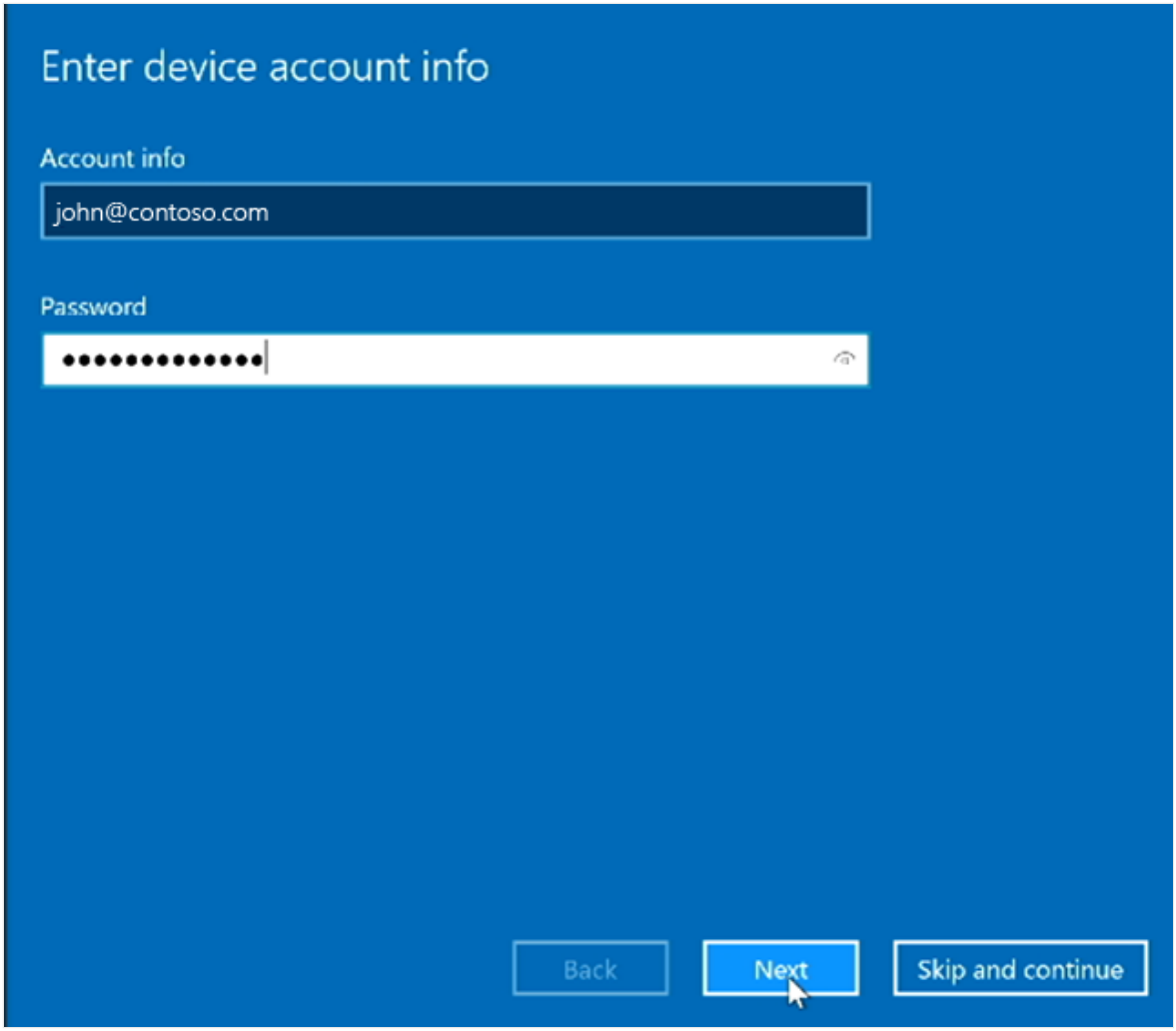
5. **Connect to a network.** If you have already attached an Ethernet cable, Surface Hub automatically connects to your network. Alternatively, you can connect to a wireless network. **Note:** You cannot connect to a wireless network in hotspots (captive portals) that redirect sign-in requests to a provider's website. Select **Next**.



6. **Accept Windows 10 License Agreement.** Select **Accept**.



7. **Enter Device account info** using either a UPN address (user@contoso.com) or a down-level domain address (CONTOSO\user). Use the format that matches your environment and enter the password.

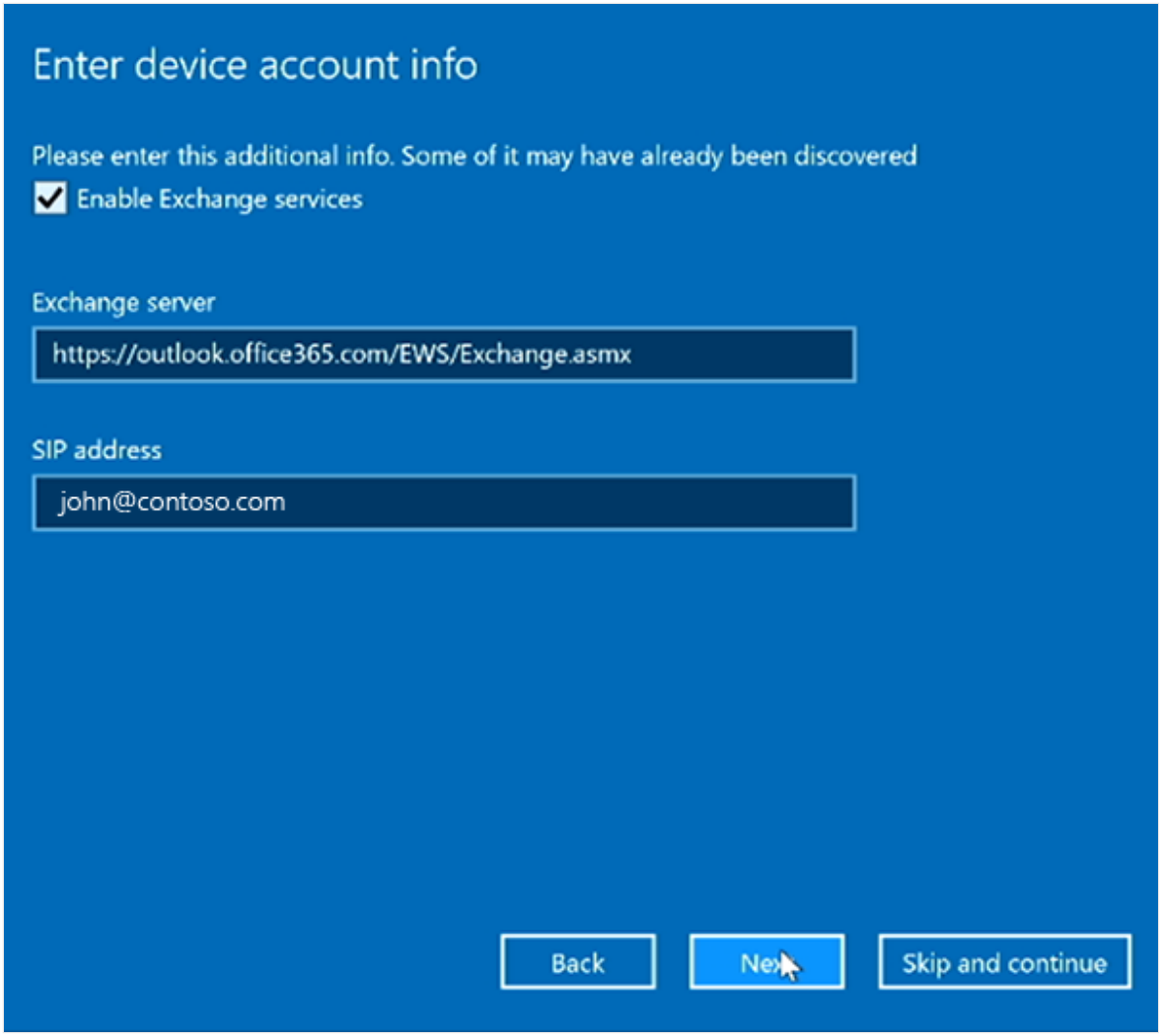


Environment	Required format for device account
Device account is hosted only online	username@contoso.com
Device account is hosted only on-premises	CONTOSO\user
Device account is hosted online and on-premises (hybrid)	CONTOSO\user

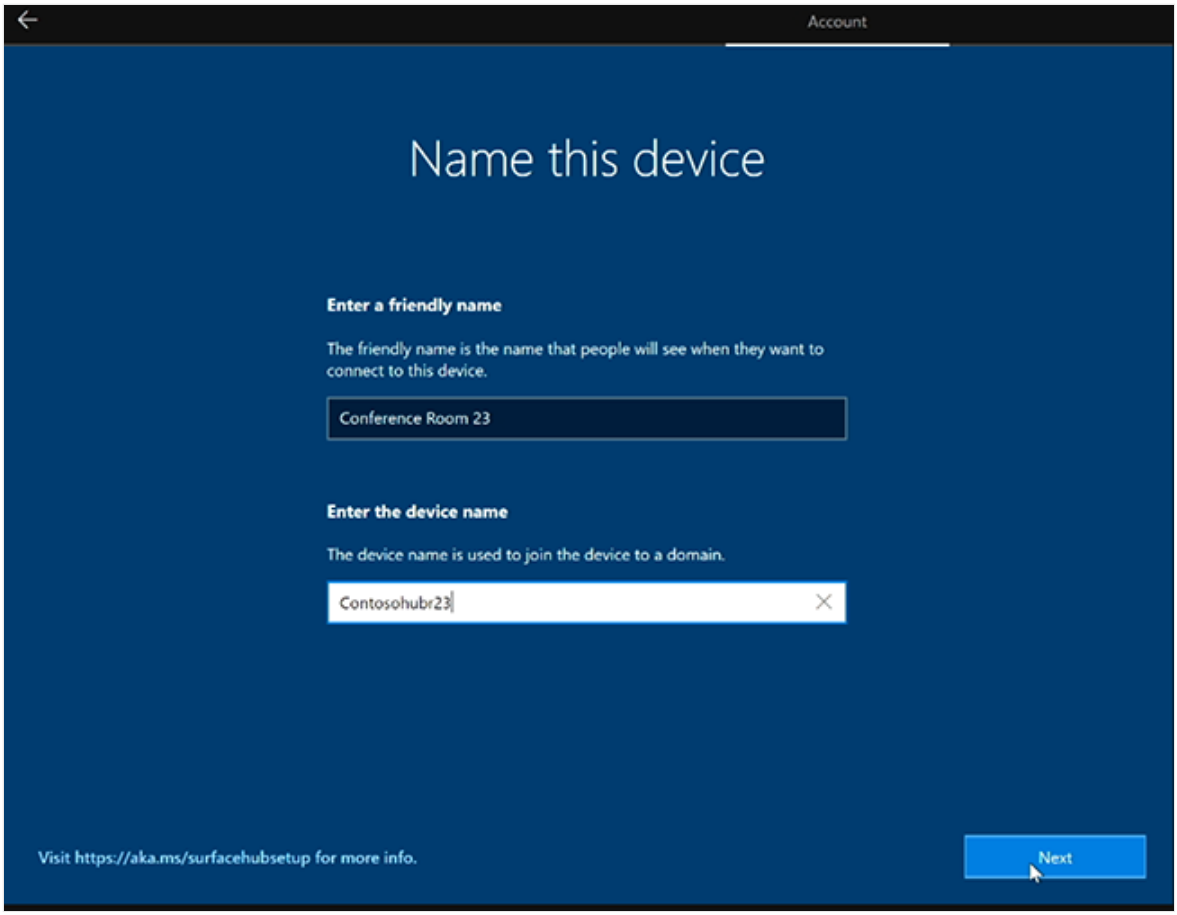
> ⓘ **Note**
>
> Although you can skip setting up a device account, the device will not be fully integrated into your infrastructure. If you skip setting it up now, you can add a device account later by using the Settings app.

8. **Enter your password** and select **Next**.

9. Surface Hub automatically detects Exchange server and SIP address info from the domain entered in the previous step. Or if needed, provide your Exchange server address and select **Next**.



10. **Name this device.** Enter a name for your device or use the suggested one. **Select Next**.



- The **Friendly name** is visible on the bottom left corner of Surface Hub 2S and is shown when projecting to the device.
- The **Device name** identifies the device when affiliated with Active Directory or Azure Active Directory, and when enrolling the device with Intune.

> **Important**
>
> If you plan to affliate the Surface Hub with Active Directory, the device name must meet the **standard requirements for computer names in AD**, otherwise setup will fail.

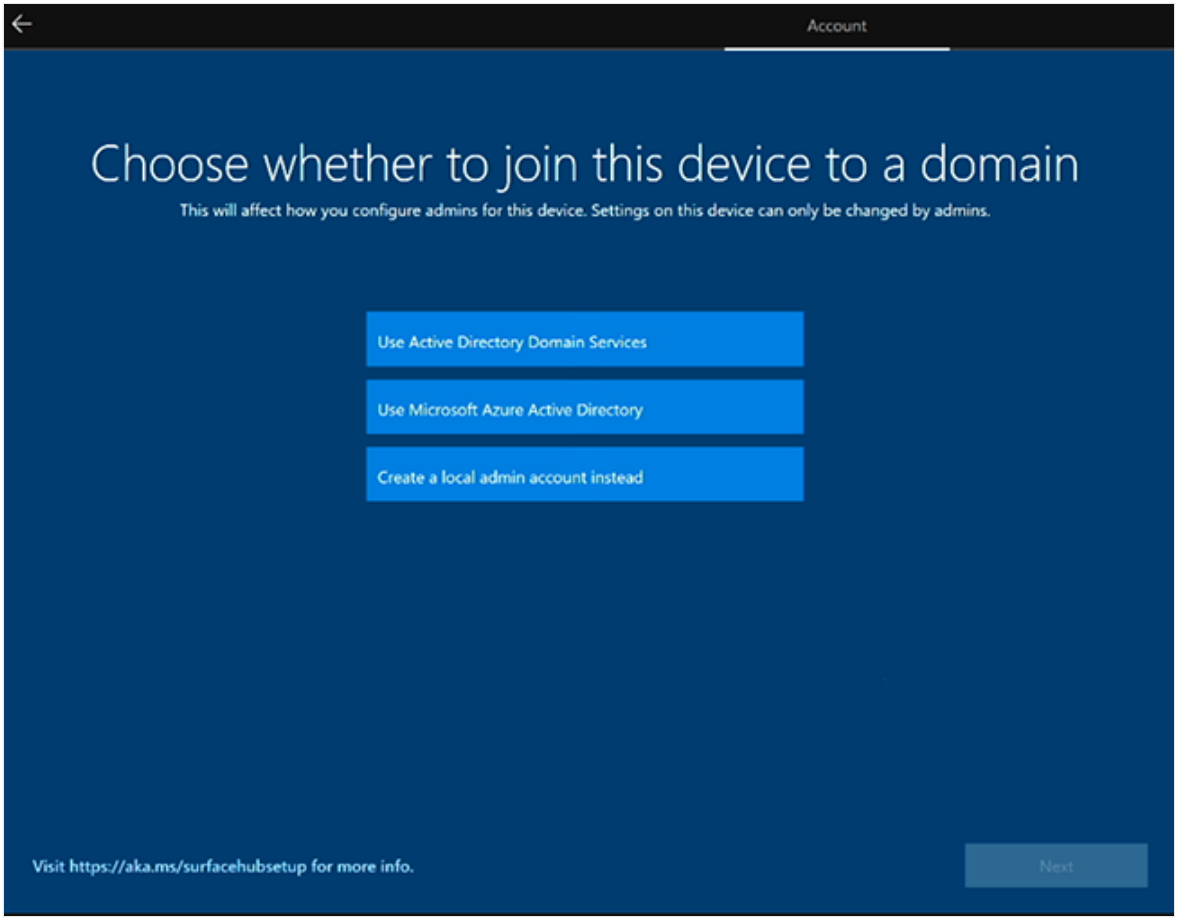
> **Tip**
>
> If you want to enable **Miracast over Infrastructure**, the device name needs to be discoverable via DNS. You can achieve this by either allowing your Surface Hub to register automatically via Dynamic DNS, or by manually creating an A or AAAA record for the Surface Hub's device name.

Configure device admin accounts

You can only set up device admins during first time Setup. For more information, refer to:

- Surface Hub 2S device affiliation
- Admin Group Management

1. **Choose type of admin account.** Select one of the following options: Active Directory Domain Services, Azure Active Directory, or Local admin.



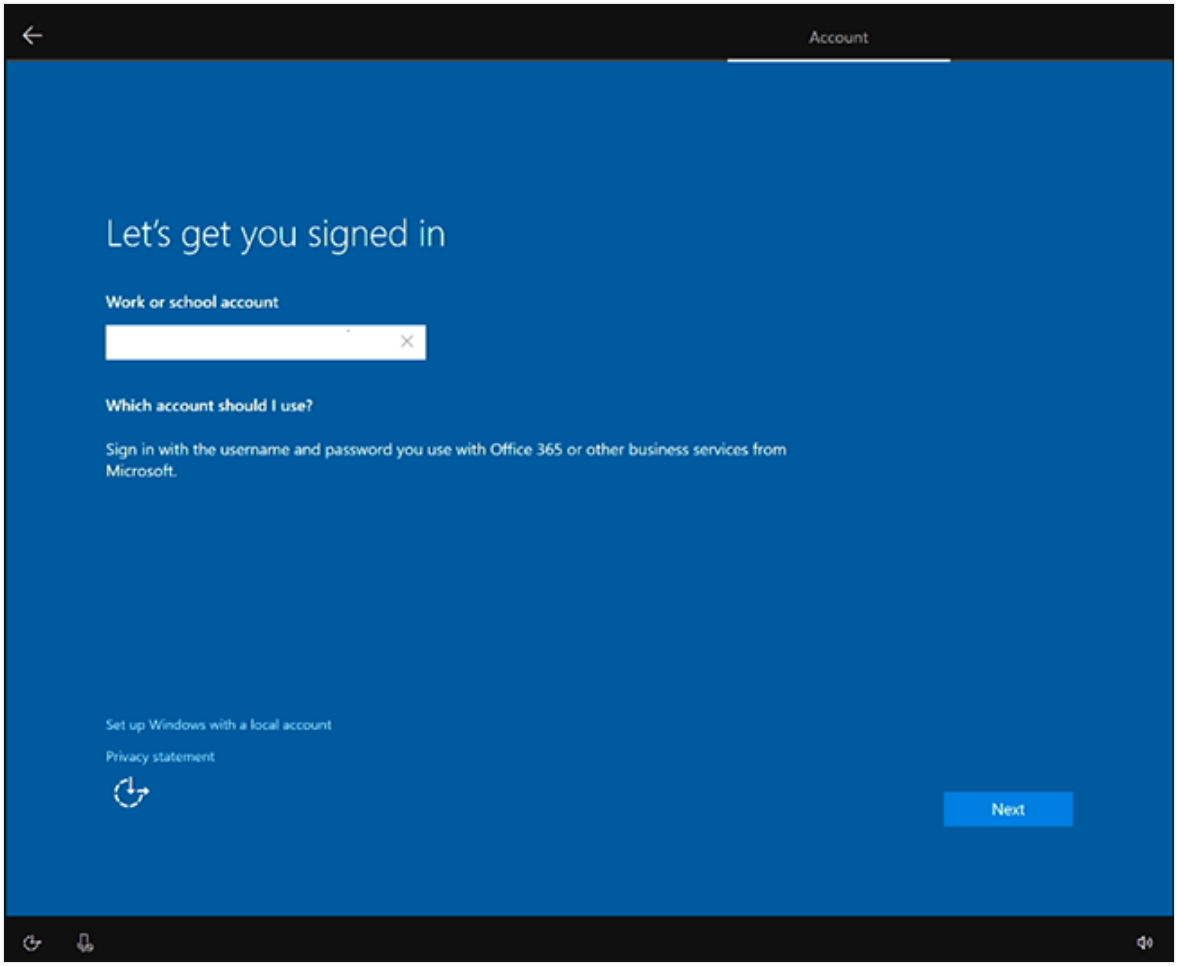
Active Directory Domain Services

1. If you intend to use Surface Hub in an on-premises environment, you can affiliate Hub with **Active Directory Domain Services**. Enter the credentials of a user who has permissions to join the device to Active Directory.
2. Select the Active Directory Security Group containing members allowed to sign in to the Settings app on Surface Hub 2S.
3. Select **Finish**. The device will restart.

Microsoft Azure Active Directory

1. If you intend to manage Surface Hub from the cloud using Microsoft Intune or an MDM provider, select **Microsoft Azure Active Directory**.

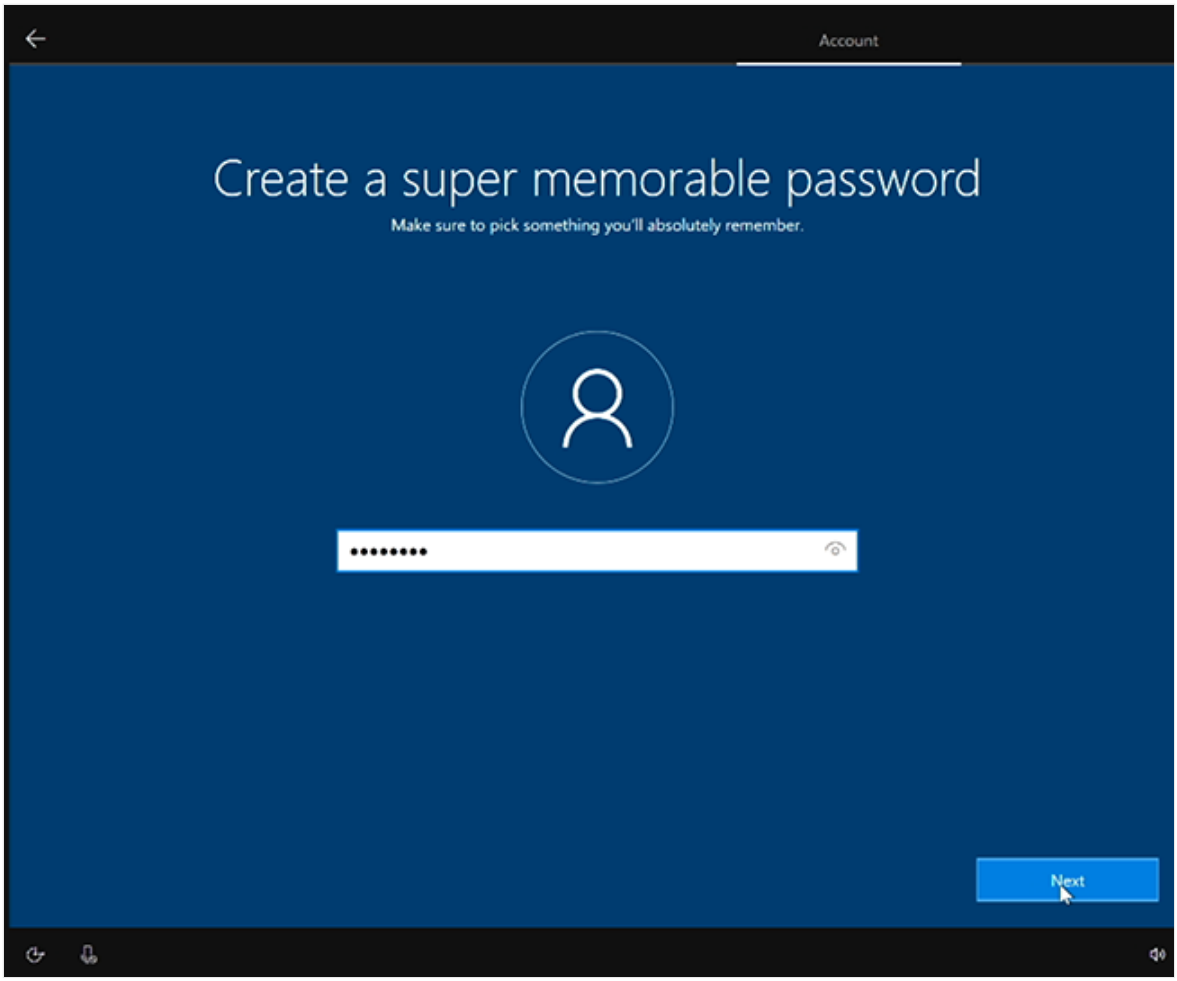
2. Select Next and sign in with a work or school account. If redirected, authenticate using your organization's sign-in page and provide additional credentials if requested. Otherwise, enter your password and select **Next.**



> **Tip**
>
> To configure who can use the Settings app to manage Surface Hubs, ensure that automatic Intune enrollment is enabled in your tenant before joining the device to Azure AD. Intune policies can then be used to **configure non-Global admins** on Surface Hubs.

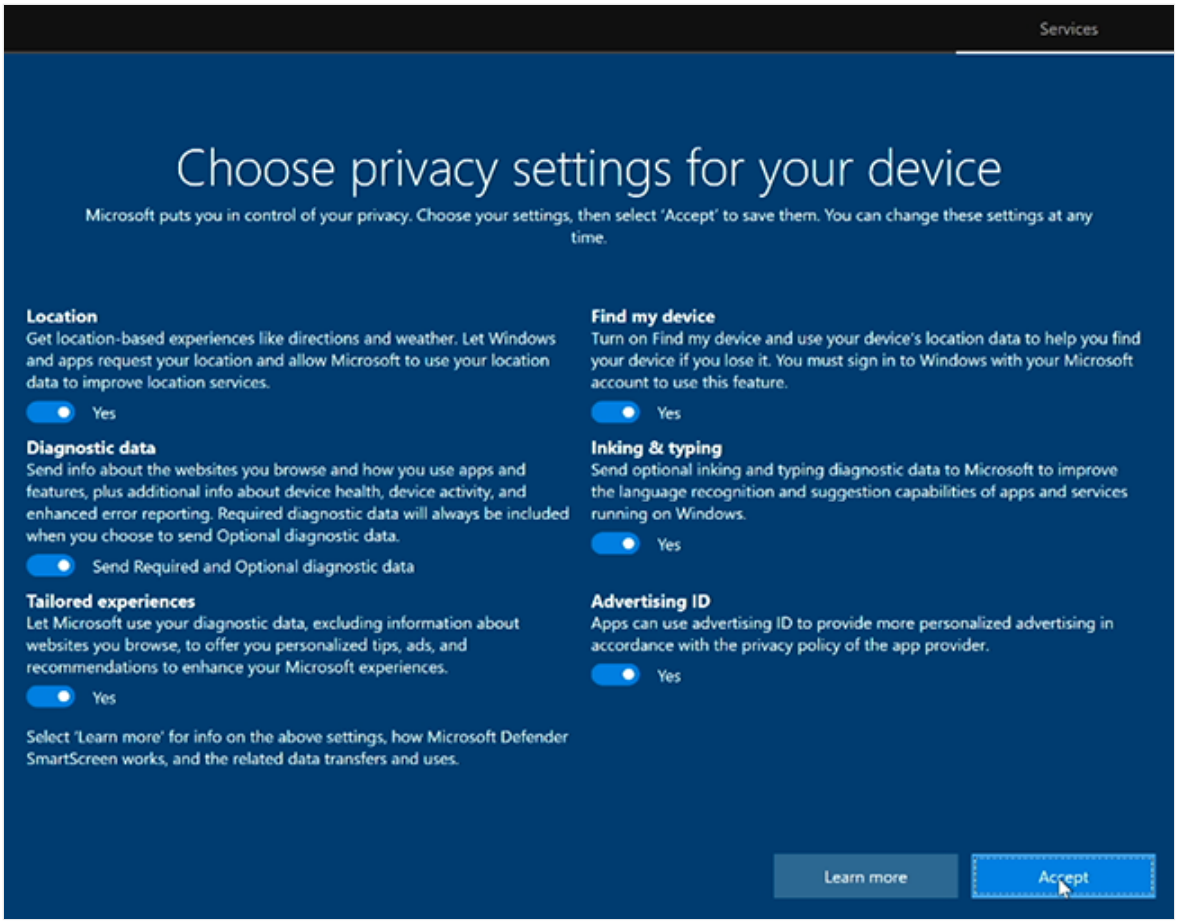
Local Administrator account

- Enter a username and a memorable password for your local admin. (If you forget the local admin password you will need to recover your device and repeat the setup process.)



Choose privacy settings for your device

- Select from the available privacy settings and select **Accept.**



Use provisioning packages

You can customize first time setup options, allowing you to ensure a consistent experience across multiple Surface Hubs.

1. To begin, review the documentation in Create provisioning packages and save the provisioning package to a USB thumb drive.
2. Insert the USB thumb drive into one of the USB ports when you see the License Agreement page (step 6 in the "Get started" steps above).
3. When prompted, choose the provisioning package you'd like to use.
4. Follow the rest of the steps, and remove the USB drive at the first reboot that occurs in the setup process.

Learn more

- Prepare your environment for Surface Hub
- Surface Hub and Microsoft Teams Rooms automated setup guide

Admin group management for Surface Hub

Article • 01/10/2023 • Applies to: Surface Hub, Surface Hub 2S

Every Surface Hub can be configured locally using the Settings app on the device. To prevent unauthorized users from changing settings, the Settings app requires admin credentials to open the app.

Admin Group Management

You can set up administrator accounts for the device in the following ways:

- Create a local admin account
- Domain join the device to Active Directory
- Azure AD join the device
- Configure non-Global Admin accounts on Azure AD joined devices (Surface Hub 2S)

Create a local admin account

To create a local admin, choose to use a local admin during first run. This will create a single local admin account on the Surface Hub with the username and password of your choice. Use these credentials to open the Settings app.

Note that the local admin account information is not backed by any directory service. We recommend you only choose a local admin if the device does not have access to Active Directory (AD) or Azure Active Directory (Azure AD). If you decide to change the local admin's password, you can do so in Settings. However, if you want to change from using the local admin account to using a group from your domain or Azure AD tenant, then you'll need to reset the device and go through the first-time program again.

Domain join the device to Active Directory

You can domain join the Surface Hub to your AD domain to allow users from a specified security group to configure settings. During first run, choose to use Active Directory Domain Services. You'll need to provide credentials that are capable of joining the domain of your choice, and the name of an existing security group. Anyone who is a member of that security group can enter their credentials and unlock Settings.

What happens when you domain join your Surface Hub?

Surface Hubs use domain join to:

- Grant admin rights to members of a specified security group in AD.
- Backup the device's BitLocker recovery key by storing it under the computer object in AD. See Save your BitLocker key for details.
- Synchronize the system clock with the domain controller for encrypted communication

Surface Hub does not support applying Group Policy or certificates from the domain controller.

> **Note**
>
> If your Surface Hub loses trust with the domain (for example, if you remove the Surface Hub from the domain after it is domain joined), you won't be able to authenticate into the device and open up Settings. If you decide to remove the trust relationship of the Surface Hub with your domain, **reset the device** first.

Azure AD join the device

You can Azure Active Directory (Azure AD) to join the Surface Hub to allow IT pros from your Azure AD tenant to configure settings. During first run, choose to use Microsoft Azure Active Directory. You will need to provide credentials that are capable of joining the Azure AD tenant of your choice. After you successfully Azure AD join, the appropriate people will be granted admin rights on the device.

By default, all **global administrators** will be given admin rights on an Azure AD joined Surface Hub. With **Azure AD Premium** or **Enterprise Mobility Suite (EMS)**, you can add additional administrators:

1. In the Azure classic portal, click **Active Directory**, and then click the name of your organization's directory.
2. On the **Configure** page, under **Devices** > **Additional administrators on Azure AD joined devices**, click **Selected**.
3. Click **Add**, and select the users you want to add as administrators on your Surface Hub and other Azure AD joined devices.
4. When you have finished, click the checkmark button to save your change.

What happens when you Azure AD join your Surface Hub?

Surface Hubs use Azure AD join to:

- Grant admin rights to the appropriate users in your Azure AD tenant.
- Backup the device's BitLocker recovery key by storing it under the account that was used to Azure AD join the device. See Save your BitLocker key for details.

Automatic enrollment via Azure Active Directory join

Surface Hub now supports the ability to automatically enroll in Intune by joining the device to Azure Active Directory.

For more information, see Set up enrollment for Windows devices.

Which should I choose?

If your organization is using AD or Azure AD, we recommend you either domain join or Azure AD join, primarily for security reasons. People will be able to authenticate and unlock Settings with their own credentials, and can be moved in or out of the security groups associated with your domain.

Option	Requirements	Which credentials can be used to access the Settings app?
Create a local admin account	None	The user name and password specified during first run
Domain join to Active Directory (AD)	Your organization uses AD	Any AD user from a specific security group in your domain
Azure Active Directory (Azure AD) join the device	Your organization uses Azure AD Basic	Global administrators only
	Your organization uses Azure AD Premium or Enterprise Mobility Suite (EMS)	Global administrators and additional administrators

Configure non-Global Admin accounts on Azure AD-joined devices

For Surface Hub v1 and Surface Hub 2S devices joined to Azure AD, Windows 10 Team 2020 Update lets you limit admin permissions to management of the Settings app on Surface Hub. This enables you to scope admin permissions for Surface Hub only and

prevent potentially unwanted admin access an entire Azure AD domain. To learn more, see Configure non-Global Admin accounts on Surface Hub.

Setup worksheet (Surface Hub)

Article • 01/10/2023 • Applies to: Surface Hub, Surface Hub 2S

When you've finished pre-setup and are ready to start first-time setup for your Microsoft Surface Hub, make sure you have all the information listed in this section.

You should fill out one list for each Surface Hub you need to configure, although some information can be used on all Surface Hubs, like the proxy information or domain credentials. Some of this information may not be needed, depending on how you've decided to configure your device, or depending on how the environment is configured for your organization's infrastructure.

When finished, review Post deployment checklist below.

Property	What this is used for	Example	Learn more
Proxy information	If you use a proxy for network or Internet access, you must provide a script or server/port information.	Proxy script: http://contoso/proxy.pac Or: Server and port info: 10.10.10.100, port 80	Configure proxy using provisioning package.
Wireless network credentials (username and password)	If connecting your device to Wi-Fi, and your wireless network requires user credentials.	admin1@contoso.com, #MyPassw0rd	Wireless network management
Device account UPN or Domain\username and device account password	This is the User Principal Name (UPN) or the domain\username, and the password of the device account. Mail, calendar, Microsoft Teams, and Skype for Business depend on a compatible device account.	UPN: ConfRoom15@contoso.com, #Passw0rd1 Or: Domain and username: CONTOSO\ConfRoom15, #Passw0rd1	Create and test a device account
Mailbox properties	The mailbox must be configured with the correct properties to enable the best meeting experience on Surface Hub.	See Microsoft Exchange properties	

Property	What this is used for	Example	Learn more
EWS URL for device account's mailbox	This is the device account's Exchange server. Mail, calendar, Microsoft Teams, and Skype for Business depend on a compatible device account. For mail and calendaring to work, the device account must have a valid Exchange server. The device will try to find this automatically.	https://outlook.office365.com/EWS/exchange.asmx	Create and test a device account Microsoft Exchange properties
Device account Session Initiation Protocol (SIP) address	This is the device account's SIP address. Mail, calendar, Microsoft Teams, and Skype for Business depend on a compatible device account. For Teams or Skype for Business to work, the device account must have a valid SIP address. The device will try to find this automatically.	sip: ConfRoom15@contoso.com	

Property	What this is used for	Example	Learn more
Device account password	To simplify management, you can either disable password expiration for the device account or allow Surface Hub to automatically rotate the device account password. **Note:** If adding the account in domain\username format, affiliate the Hub with on-premises Active Directory during initial setup. If adding the account in username@domain.com format, affiliate the Hub with Azure Active Directory during initial setup. Otherwise, password rotation will not work.		Password management
Exchange Web Services (EWS)	Enable EWS. Surface Hub uses EWS to sync its calendar.		Modern authentication on Surface Hub
Multifactor authentication	Disable multifactor authentication on the device account. As the Surface Hub logs into Exchange in the background without user interaction, it cannot respond to any interactive prompts, such as multifactor authentication.		
MDM enrollment details	If you would like to manually enroll the device to MDM, you will need to have user credentials that are valid for the MDM provider and the enrollment URL. The device will try to find the enrollment URL automatically.	manage.microsoft.com	Manage Surface Hub with an MDM provider

Property	What this is used for	Example	Learn more
Friendly name	The friendly name of the device is the broadcast name that people will see when they try to wirelessly connect to the Surface Hub. This name will be displayed prominently on the Surface Hub's screen. We suggest that the friendly name you choose is recognizable and unique so that people can distinguish one Surface Hub from another when trying to connect.	Conference Room 15	First time Setup for Surface Hub
Device name	The device name is the name that will be used for domain join, and is the identity you will see in your MDM provider if the device is enrolled into MDM. The device name you choose must not be the same name as any other device in your Active Directory domain (if you decide to domain join the device). The device cannot join the domain without a unique name.	confroom15	First time Setup for Surface Hub
Teams App Mode	- Mode 0 — Skype for Business with Microsoft Teams functionality for scheduled meetings. - Mode 1 — Microsoft Teams only		Changing default app for meetings & calls

Device affiliation

Use Device affiliation to manage user access to the Settings app on Surface Hub. With the Windows 10 Team operating system (that runs on Surface Hub), only authorized users can adjust settings using the Settings app. Since choosing the affiliation can impact feature availability, plan appropriately to ensure that users can access features as intended.

> ⓘ **Note**

You can only set Device affiliation during the initial out-of-box experience (OOBE) setup. If you need to reset Device affiliation, you'll have to repeat OOBE setup.

If you're joining Azure AD

Property	What this is used for	Example	Learn more
Azure AD tenant user credentials (username and password)	If you decide to have people in your Azure Active Directory (Azure AD) organization become admins on the device, then you'll need to join the Surface Hub to Azure AD. To join it to Azure AD, you will need valid credentials for an account in the tenant.	admin1@contoso.com, #MyPassw0rd	Admin group management
Non Global Admin accounts	For Surface Hub devices joined to Azure AD, you can limit admin permissions to management of the Settings app on Surface Hub. This enables you to scope admin permissions for Surface Hub only and prevent potentially unwanted admin access an entire Azure AD domain.		Configure non-Global Admin accounts on Surface Hub

If you're joining a domain

Property	What this is used for	Example
Domain to join	This is the domain you will need to join so that a security group of your choice can be admins for the device. You may need the fully qualified domain name (FQDN).	contoso (short name) OR contoso.corp.com (FQDN)
Domain account credentials (username and password)	A domain can't be joined unless you provide sufficient account credentials to join the domain. Once you provide a domain to join and credentials to join the domain, then a security group of your choice can change settings on the device.	admin1, #MyPassw0rd
Admin security group alias	This is a security group in your Active Directory (AD); any members of this security group can change settings on the device.	SurfaceHubAdmins

If you're using a local admin

Property	What this is used for	Example
Local admin account credentials (username and password)	If you decide not to join an AD domain or Azure AD, you can create a local admin account on the device.	admin1, #MyPassw0rd

If you need to install certificates or apps

Property	What this is used for
USB drive	If you know before first run that you want to install certificates or universal apps, follow the steps in Create provisioning packages for Surface Hub. Your provisioning packages will be created on a USB drive.

Post deployment checklist

Check	Response
Device account syncing	☐ Yes ☐ No
Bitlocker key	☐ Saved to file (no affiliation) ☐ Saved in Active Directory (AD affiliation) ☐ Saved in Azure AD (Azure AD affiliation)
Device OS updates	☐ Completed
Windows Store updates	☐ Automatic ☐ Manual
Microsoft Teams scheduled meeting	☐ Confirmation email received ☐ Meeting appears on start screen ☐ One-touch join functions ☐ Able to join audio ☐ Able to join video ☐ Able to share screen
Skype for Business scheduled meeting	☐ Confirmation email received ☐ Meeting appears on start screen ☐ One-touch join functions correctly ☐ Able to join audio ☐ Able to join video ☐ Able to share screen ☐ Able to send/receive IM
Scheduled meeting when already invited	☐ Meeting declined

Check	Response
Microsoft Teams ad-hoc meeting	☐ Invite other users work ☐ Able to join audio ☐ Able to join video ☐ Able to share screen
Microsoft Whiteboard	☐ Launch from Welcome / Start screen ☐ Launch from Microsoft Teams
Incoming Teams/Skype call	☐ Able to join audio ☐ Able to join video ☐ Able to share screen ☐ Able to send/receive IM (Skype for Business only)
Incoming live video streams	☐ Maximum 2 (Skype for Business) ☐ Maximum 4 (Microsoft Teams)
Microsoft Teams Mode 0 behavior	☐ Skype for Business tile on Welcome/Start screen ☐ Can join scheduled Skype for Business meetings (Skype UI) ☐ Can join scheduled Teams meetings from Welcome screen calendar
Microsoft Teams Mode 1 behavior	☐ Teams tile on Welcome / Start screen ☐ Can join scheduled Teams meetings ☐ Cannot join Skype for Business meetings

Prepare your environment for Surface Hub

Article • 01/27/2023 • Applies to: Surface Hub, Surface Hub 2S

This page describes dependencies for setting up and managing Surface Hub v1 or Surface Hub 2S.

> **Tip**
>
> As a companion to this article, we recommend using the **Surface Hub and Microsoft Teams Rooms automated setup guide** when signed in to the Microsoft 365 Admin Center. This guide will customize your experience based on your environment. If you're hosted in Exchange Online and using Microsoft Teams, the guide will automatically create your device account with the correct settings. Or use it to validate existing resource accounts to help turn them into compatible Surface Hub device accounts. To review best practices without signing in and activating automated setup features, go to the **M365 Setup portal**.

Infrastructure dependencies

Review these dependencies to make sure Surface Hub features will work in your IT infrastructure.

Dependency	Description	Learn more
On-premises services and Active Directory or M365	Surface Hub uses an Active Directory or Azure AD account (called a **device account**) to access Exchange and Teams (or Skype for Business) services. The Surface Hub must be able to connect to your Active Directory domain controller or to your Azure AD tenant in order to validate the device account's credentials, as well as to access information like the device account's display name, alias, Exchange server, and Session Initiation Protocol (SIP) address. **NOTE: Surface Hubs work with Microsoft Teams, Skype for Business Server 2019, Skype for Business Server 2015, or Skype for Business Online. Earlier platforms, such as Lync Server 2013, are not supported. Surface Hubs are not supported in GCC DoD environments.**	Microsoft 365 endpoints Create and test a device account

Dependency	Description	Learn more
Windows Update, Store and Diagnostics	Access to Windows Update or Windows Update for Business is required to maintain Surface Hub with OS feature and quality updates. Access to the Microsoft Store is required to maintain apps.	Manage connection endpoints for Windows 10 Enterprise, version 20H2 Manage Windows updates on Surface Hub
Mobile device management (MDM) solution (Microsoft Intune, Microsoft Endpoint Configuration Manager, or supported third-party MDM provider)	If you want to apply settings and install apps remotely, and to multiple devices at a time, you must set up an MDM solution and enroll the device to that solution.	Network endpoints for Microsoft Intune Manage settings with an MDM provider
Azure Monitor	Azure Monitor can be used to monitor the health of Surface Hub devices. **NOTE: Surface Hubs do not currently support the use of a proxy server to communicate with the Log Analytics service utilized by Azure Monitor.**	Log Analytics endpoints Monitor Surface Hubs with Azure Monitor to track their health.

Dependency	Description	Learn more
Network access	Surface Hubs support both wired or wireless connections (a wired connection is preferred). **802.1X authentication** In Windows 10 Team 20H2, although 802.1X authentication for wired and wireless connections is enabled by default, you need to ensure that an 802.1x network profile and authentication certificate are also installed on Surface Hub. If you manage Surface Hub with Intune or other mobile device management solution, you can deliver the certificate using the ClientCertificateInstall CSP. Otherwise you can create a provisioning package and install it during first run setup or by using the Settings app. When the certificate is applied, 802.1X authentication begins automatically. **Dynamic IP** Surface Hubs cannot be configured to use a static IP. They must be assigned an IP address through DHCP. **Ports** The Surface Hub requires the following open ports: HTTPS: 443 HTTP: 80 NTP: 123	Enable 802.1x wired authentication Create provisioning packages for Surface Hub

Device affiliation

Use Device affiliation to manage user access to the Settings app on Surface Hub. With the Windows 10 Team operating system (that runs on Surface Hub), only authorized users can adjust settings using the Settings app. Since choosing the affiliation can impact feature availability, plan appropriately to ensure that users can access features as intended.

> **Note**
>
> You can only set Device affiliation during the initial out-of-box experience (OOBE) setup. If you need to reset Device affiliation, you'll have to repeat OOBE setup.

No affiliation

No affiliation is like having Surface Hub in a workgroup with a different local Administrator account on each Surface Hub. If you choose No affiliation, you must locally save the BitLocker Key to a USB thumb drive. You can still enroll the device with Intune; however, only the local admin can access the Settings app using the account credentials configured during OOBE. You can change the Administrator account password from the Settings app.

Active Directory Domain Services

If you affiliate Surface Hub with on-premises Active Directory Domain Services, you need to manage access to the Settings app using a security group on your domain. This helps ensure that all security group members have permissions to change settings on Surface Hub. Also note the following: When Surface Hub affiliates with your on-premises Active Directory Domain Services, the BitLocker key can be saved in the Active Directory Schema. For more information, see Prepare your organization for BitLocker: Planning and policies.

Your organization's Trusted Root CAs are pushed to the same container in Surface Hub, which means you don't need to import them using a provisioning package.

You can still enroll the device with Intune to centrally manage settings on your Surface Hub.

Azure Active Directory

When you choose to affiliate your Surface Hub with Azure Active Directory (Azure AD), any user with the Global Administrator role can sign in to the Settings app on Surface Hub. You can also configure non-Global Admin accounts that limit permissions to management of the Settings app on Surface Hub. This enables you to scope admin permissions for Surface Hubs only and prevent potentially unwanted admin access across an entire Azure AD domain.

> ⓘ **Note**
>
> Surface Hub administrator accounts can only sign in to the Settings app when **authenticating via Azure AD**. Third-party federated Identity Providers (IdPs) are not supported.

If you enabled Intune Automatic Enrollment for your organization, the Surface Hub will automatically enroll itself with Intune; in this scenario, the account used for Azure AD affiliation during setup must be licensed for Intune and have permissions to enroll

Windows devices. After the setup process is completed, the device's BitLocker key is automatically saved in Azure AD.

To learn more about managing Surface Hub with Azure AD, see:

- Admin group management
- Configure non-Global Admin accounts on Surface Hub

Review and complete Surface Hub setup worksheet (optional)

When you go through the first-run program for your Surface Hub, there's some information that you'll need to supply. The setup worksheet summarizes that info, and provides lists of environment-specific info that you'll need when you go through the first-run program. For more information, see Setup worksheet.

Learn more

- Surface Hub and Microsoft Teams Rooms automated setup guide

Save your BitLocker key (Surface Hub)

Article • 02/16/2023 • Applies to: Surface Hub, Surface Hub 2S

Every Microsoft Surface Hub is automatically set up with BitLocker drive encryption software. Microsoft strongly recommends that you make sure you back up your BitLocker recovery keys.

There are several ways to manage your BitLocker key on the Surface Hub.

1. If you've joined the Surface Hub to a domain, the device will back up the key on the domain and store it under the computer object.

   If you can't find the BitLocker key after joining the device to a domain, it's likely that your Active Directory schema doesn't support BitLocker key backup. If you don't want to change the schema, you can save the BitLocker key by going to Settings and following the procedure for using a local admin account, which is detailed later in this list.

2. If you've joined the Surface Hub to Azure Active Directory (Azure AD), the BitLocker key will be stored under the account that was used to join the device.

3. If you're using a local admin account to manage the device, you can save the BitLocker key by going to the **Settings** app and navigating to **Update & security** > **Recovery**. Insert a USB drive and select the option to save the BitLocker key. The key will be saved to a text file on the USB drive.

Related topics

- Manage Microsoft Surface Hub
- Microsoft Surface Hub administrator's guide

Create and test a device account on Surface Hub

Article • 03/27/2023

Creating a Surface Hub device account (also known as a resource account/room mailbox) allows the Surface Hub to receive, approve, or decline meeting requests and join meetings.

Once the device account is provisioned on a Surface Hub, people can add this account to a meeting invitation the same way that they would invite a conference room.

You can configure the device account during the Out-of-Box Experience (OOBE) setup. If needed, you can also change it later in **Settings** > **Surface Hub** > **Accounts**.

> **Tip**
>
> As a companion to this article, we recommend using the **Surface Hub and Microsoft Teams Rooms automated setup guide** when signed in to the Microsoft 365 Admin Center. This guide will customize your experience based on your environment. If you're hosted in Exchange Online and using Microsoft Teams, the guide will automatically create your device account with the correct settings. Or use it to validate existing resource accounts to help turn them into compatible Surface Hub device accounts. To review best practices without signing in and activating automated setup features, go to the **M365 Setup portal**.

Configuration overview

This table explains the main steps and configuration decisions when you create a device account.

Step	Description	Purpose

Step	Description	Purpose
1	Create a logon-enabled room mailbox (Exchange Online or Exchange Server 2016 and later)	This type of mailbox allows the device to maintain a meeting calendar, receive meeting requests, and send mail. It must be logon-enabled in order to be used with a Surface Hub.
2	Configure mailbox properties	The mailbox must be configured with the correct properties to enable the best meeting experience on Surface Hub. For more information on mailbox properties, see Mailbox properties.
3	Ensure that Exchange Web Services (EWS) is enabled, and multi-factor authentication (MFA) is disabled	The Surface Hub uses EWS to sync its calendar. If you don't allow EWS in your environment by default, the Hub mailbox would need to have it explicitly enabled. As the Surface Hub logs into Exchange in the background without user interaction, it can't respond to any interactive prompts, such as MFA. The device account you create must be excluded from any such authentication requirements. Otherwise, Surface Hub can't sync mail and calendar info.
4	Enable the account for Teams or Skype for Business (Skype for Business Server 2015 and later)	Skype for Business or Teams must be enabled to use conferencing features like video calls and screen sharing. For more information on the licenses that enable Teams, see Teams Meeting Room licensing and Teams service description. The Teams and SfB applications on the Surface Hub aren't compatible with Azure AD Conditional Access policies requiring device information (for example, compliance). The device account you create must be excluded from any such CA policies. Otherwise, Surface Hub isn't able to use any conferencing features.
5	Ensure the device account has a Teams Rooms license to meet new requirements.	Teams Rooms devices logged in with resource accounts that don't have one of the above supported Teams Rooms licenses assigned to them won't be able to sign in after July 1, 2023. - Use a sample PowerShell script to check Teams Rooms licenses on multiple devices. - To learn more, see New Microsoft Teams Rooms licensing requirements for Surface Hub
6	(Optional) Disable password expiration	To simplify management, you can turn off password expiration for the device account and allow Surface Hub to automatically rotate the device account password. For more information about password management, see Password management.

> **Note**
>
> The Surface Hub device account doesn't support third-party federated Identity Providers (IdPs) and must authenticate via Active Directory or Azure Active Directory.

Detailed configuration steps

Device account setup steps can differ based on environment. Select your deployment scenario from the following table to find the appropriate steps, and make note of the "Format to use" column for configuring Surface Hubs after the accounts are provisioned.

Organization deployment	Description	Format to use during Surface Hub setup
Online deployment (Microsoft 365)	Your organization's environment is deployed entirely on Microsoft 365.	username@domain.com
Hybrid deployment (Exchange on-premises)	Your organization has a mix of services, with Exchange Server hosted on premises and Microsoft Teams online.	username@domain.com if Hybrid Modern Authentication is enabled in Exchange, DOMAIN\username otherwise
Hybrid deployment (Exchange Online)	Your organization has a mix of services, with Skype for Business Server hosted on premises and Exchange Online.	username@domain.com if Hybrid Modern Authentication is enabled in SfB, DOMAIN\username otherwise
On-premises deployment (single forest)	Your organization has servers that it controls, where Active Directory, Exchange, and Skype for Business Server are hosted in a single-forest environment.	DOMAIN\username
On-premises deployment (multiple forests)	Your organization has servers that it controls, where Active Directory, Exchange, and Skype for Business Server are hosted in a multi-forest environment.	ACCOUNTFOREST\username

Microsoft Exchange properties for device account

Some Microsoft Exchange properties of the device account must be set to particular values to have the best meeting experience on Microsoft Surface Hub. The following table lists various Exchange properties based on PowerShell cmdlet parameters, their purpose, and the values they should be set to.

> **Tip**
>
> You can automatically configure recommended Exchange settings via the **Surface Hub and Microsoft Teams Rooms automated setup guide**.

Property	Description	Value	Impact
AutomateProcessing	The AutomateProcessing parameter enables or disables calendar processing on the mailbox.	AutoAccept	Surface Hub will be able to automatically accept or decline meeting requests based on its availability.
AddOrganizerToSubject	The AddOrganizerToSubject parameter specifies whether the meeting organizer's name is used as the subject of the meeting request.	$False	The welcome screen won't show the meeting organizer twice (instead of showing it as both the organizer and in the meeting subject).
AllowConflicts	The AllowConflicts parameter specifies whether to allow conflicting meeting requests.	$False	Surface Hub will decline meeting requests that conflict with another meeting's time.
DeleteComments	The DeleteComments parameter specifies whether to remove or keep any text in the message body of incoming meeting requests.	$False	The message body of meetings can be retained and retrieved from a Surface Hub if you need it during a meeting.
DeleteSubject	The DeleteSubject parameter specifies whether to remove or keep the subject of incoming meeting requests.	$False	Meeting request subjects can be shown on the Surface Hub.

Property	Description	Value	Impact
RemovePrivateProperty	The RemovePrivateProperty parameter specifies whether to clear the private flag for incoming meeting requests.	$False	Private meeting subjects will show as Private on the welcome screen.
AddAdditionalResponse	The AddAdditionalResponse parameter specifies whether additional information will be sent from the resource mailbox when responding to meeting requests.	$True	When a response is sent to a meeting request, custom text will be provided in the response.
AdditionalResponse	The AdditionalResponse parameter specifies the additional information to be included in responses to meeting requests. **Note** This text won't be sent unless AddAdditionalResponse is set to $True.	Your choice—the additional response can be used to inform people how to use a Surface Hub or point them towards resources.	An additional response message can provide people an introduction to how they can use a Surface Hub in their meeting.

Apply ActiveSync policies to device accounts

Surface Hubs on Windows 10 Team 1703 and earlier versions used AGctiveSync to sync mail & calendar.

The Surface Hub requirements for ActiveSync policies in your organization are as follows:

- There can't be any global policies that block synchronization of the resource mailbox that's being used by the Surface Hub's device account. If there's such a blocking policy, you need to add the Surface Hub as an allowed device.
- You must set a mobile device mailbox policy where the **PasswordEnabled** setting is set to False. Other mobile device mailbox policy settings aren't compatible with the Surface Hub.

Allowing the DeviceID

Your organization may have a global policy that prevents syncing of device accounts provisioned on Surface Hubs. To configure this property, see Allowing device IDs for ActiveSync.

Setting PasswordEnabled

The device account must have an ActiveSync policy where the **PasswordEnabled** attribute is set to False or 0. To configure this property, see Creating a Surface Hub-compatible Microsoft Exchange ActiveSync policy.

Learn more

- Prepare your environment for Surface Hub
- Surface Hub and Microsoft Teams Rooms automated setup guide
- Find Teams Rooms devices with unsupported licenses

Change the Microsoft Surface Hub device account

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

You can change the device account in Settings to accomplish the following tasks:

- Add an account if one wasn't already provisioned.
- Change any properties of an account that was already provisioned.

Device account reference

Value	Description
User Principal Name	The user principal name (UPN) of the device account.
Password	The corresponding password of the device account.
Domain	The domain that the device account belongs to. Not needed for Microsoft 365 accounts.
User name	The user name of the device account. Not needed for Microsoft 365 accounts.
Session Initiation Protocol (SIP) address	The SIP address of the device account.
Microsoft Exchange server	The Exchange server of the device account. The device account's username and password must be able to authenticate to the specified Exchange server.
Enable Exchange services	When checked, all Exchange services will be enabled (for example, calendar on the welcome screen, emailing whiteboards). When not checked, all Exchange services will be disabled, and the Exchange server doesn't need to be provided.

What happens?

The UPN and password are used to validate the account in AD or Azure AD. If the validation fails, you may need to provide the domain and user name.

Mail, calendar, Microsoft Teams, and related resources depend on a compatible device account. For Teams or Skype for Business to work, the device account must have a valid SIP address. The device will try to find the SIP automatically. If an SIP address can't be found, the UPN will be used as the SIP address. If this isn't the SIP address for the account, you'll need to provide the SIP address.

The Exchange server address will need to be provided if the device can't find a server associated with the sign-in credentials. Microsoft Surface Hub will use the Exchange server to talk to ActiveSync, which enables several key features on the device.

Related articles

- Manage Microsoft Surface Hub

Use the Surface Hub Hardware Diagnostic Tool to test a device account

Article • 01/26/2023

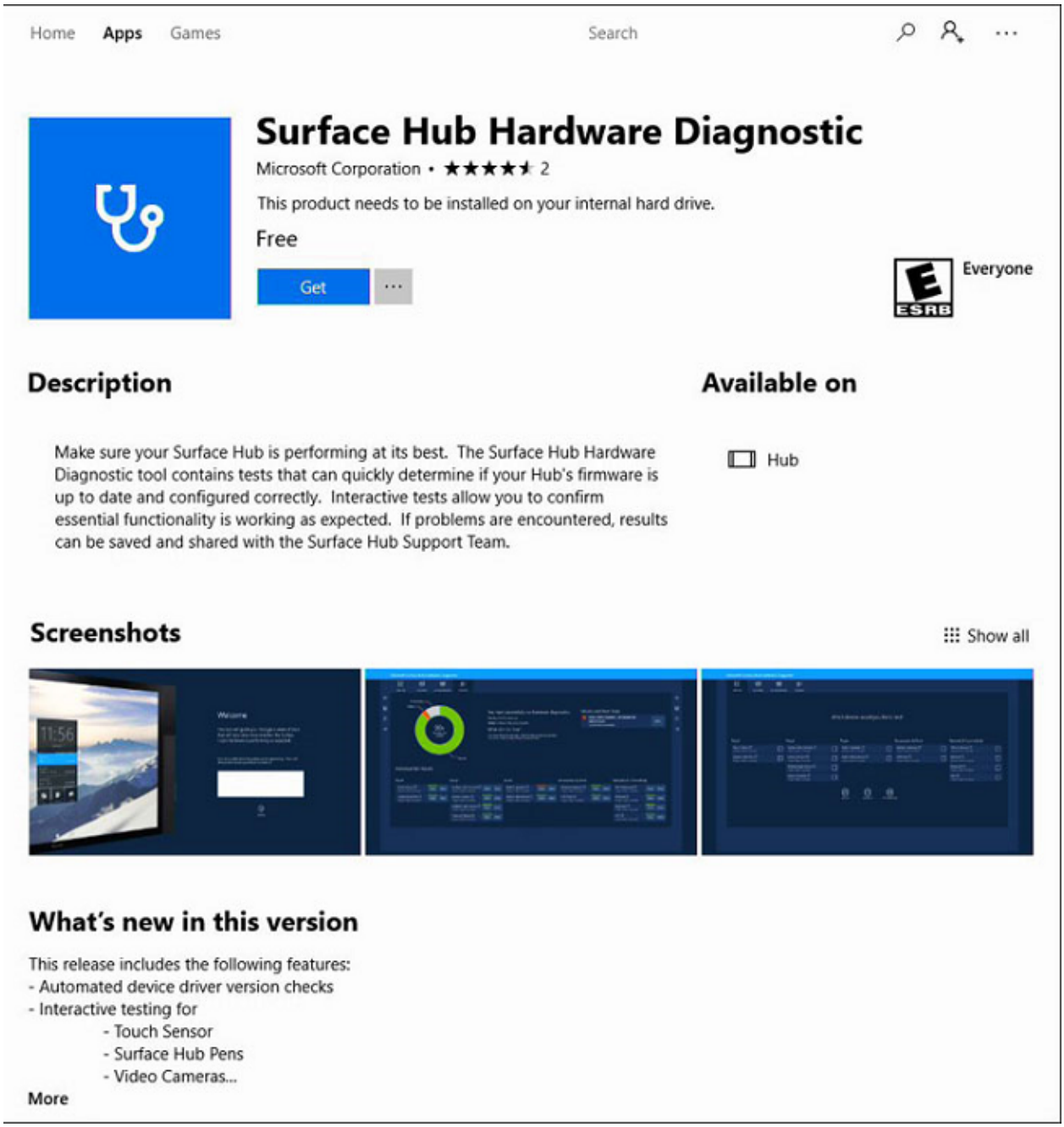
Introduction

> **Note**
>
> The "Account Settings" section of the Surface Hub Hardware Diagnostic tool doesn't collect any information. The email and password that are entered as input are used only directly on your environment and not collected or transferred to anyone. The login information persists only until the application is closed or you end the current session on the Surface Hub.

> **Important**
>
> - Administrator privileges are not required to run this application.
> - The results of the diagnostic should be discussed with your local administrator before you open a service call with Microsoft.

Surface Hub Hardware Diagnostic

By default, the Surface Hub Hardware Diagnostic application isn't installed in earlier versions of the Surface Hub system. The application is available for free from the Microsoft Store. Administrator privileges are required to install the application.



About the Surface Hub Hardware Diagnostic Tool

The Surface Hub Hardware Diagnostic tool is an easy-to-navigate tool that lets the user test many of the hardware components within the Surface Hub device. This tool can also test and verify a Surface Hub device account. This article describes how to use the Account Settings test within the Surface Hub Hardware Diagnostic tool.

> ⓘ **Note**
>
> The device account for the Surface Hub should be created before any testing is done. The Surface Hub Administrator Guide provides instructions and PowerShell scripts to help you create on-premises, online (Office365), or hybrid device

accounts. For more information, go to the **Create and test a device account (Surface Hub)** topic in the guide.

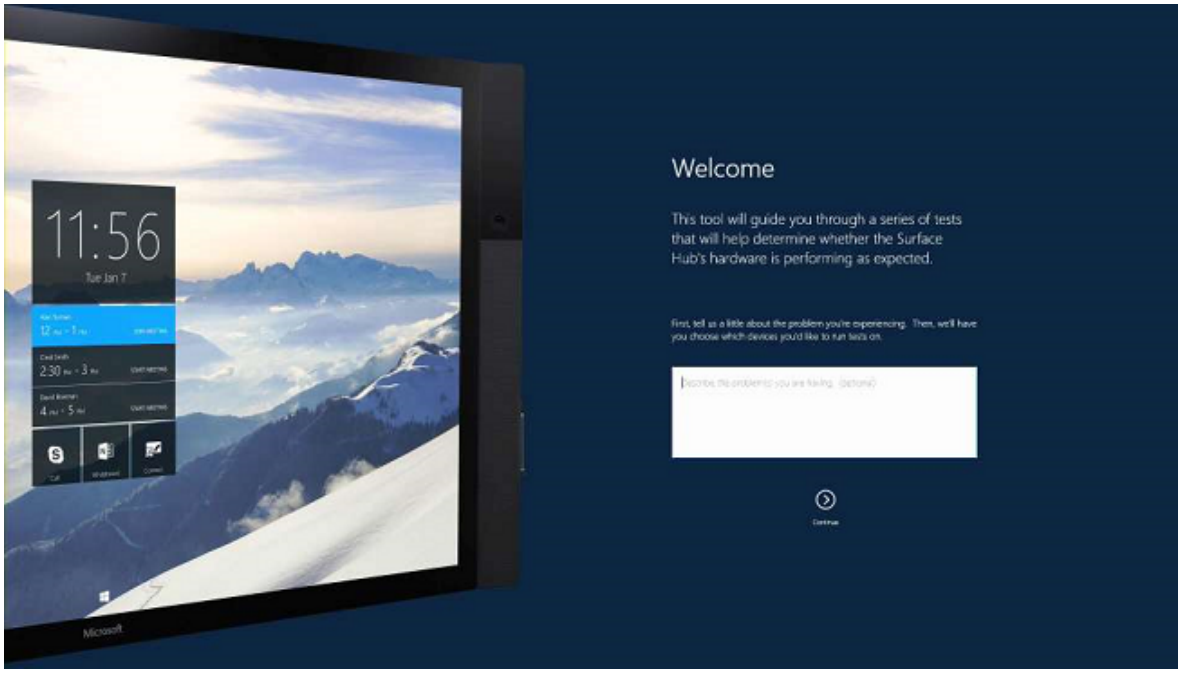
Device account testing process

1. Navigate to **All Apps**, and then locate the Surface Hub Hardware Diagnostic application.

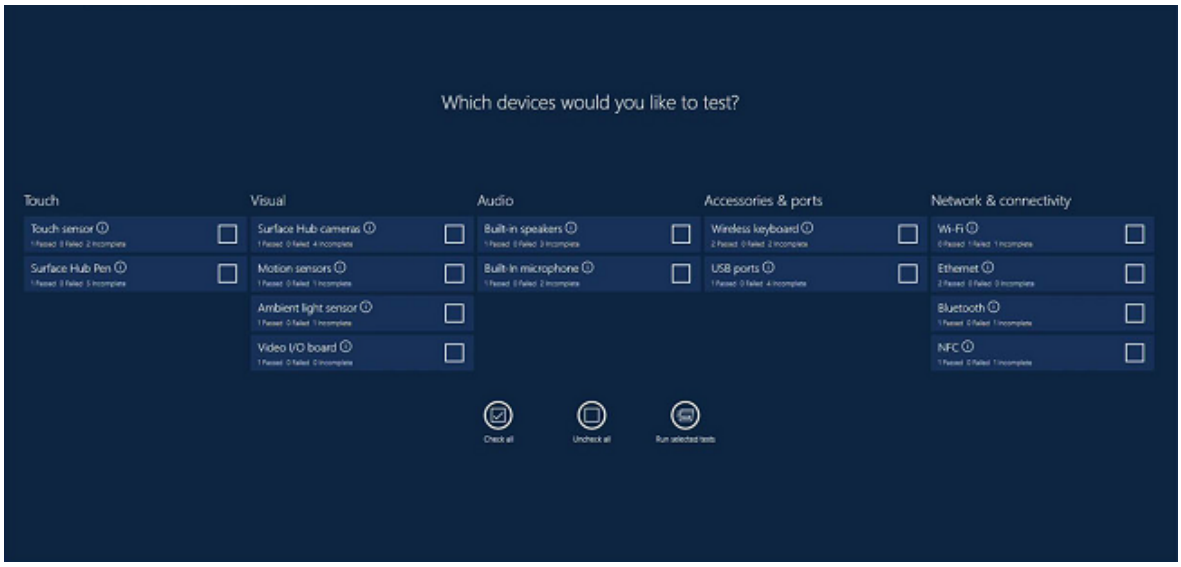
   

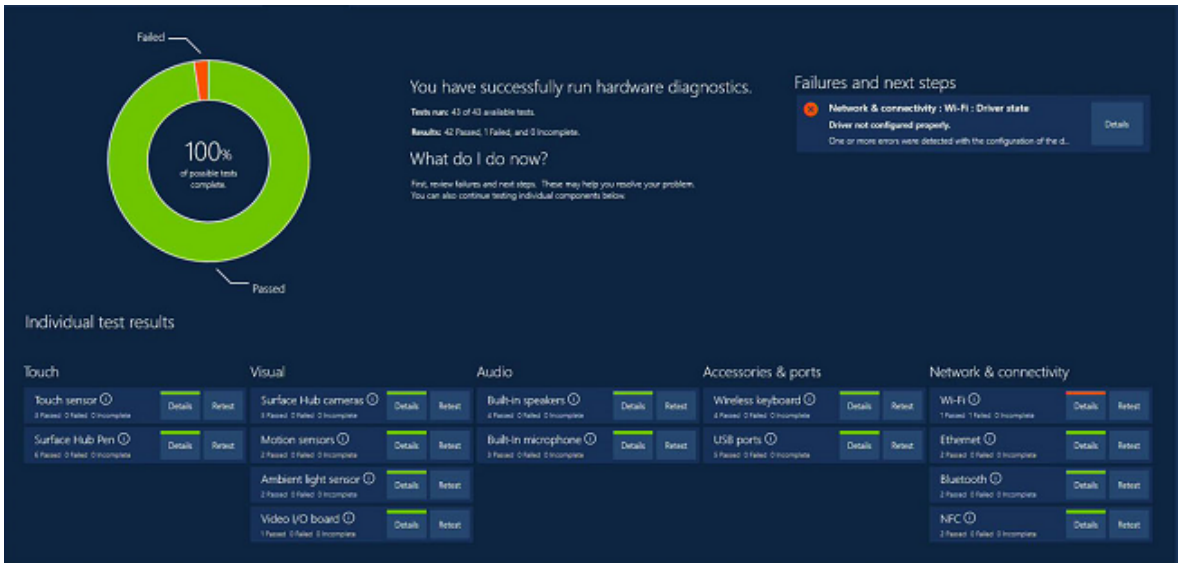
2. When the application starts, the **Welcome** page provides a text window to document the reason why you are testing the Hub. This note can be saved to USB together with the diagnostic results at the conclusion of testing. After you finish entering a note, select the **Continue** button.

   > ⓘ **Note**
   >
   > When saving diagnostic results, do not change the default path or select a subdirectory. The files can be copied later via the File Explorer app.

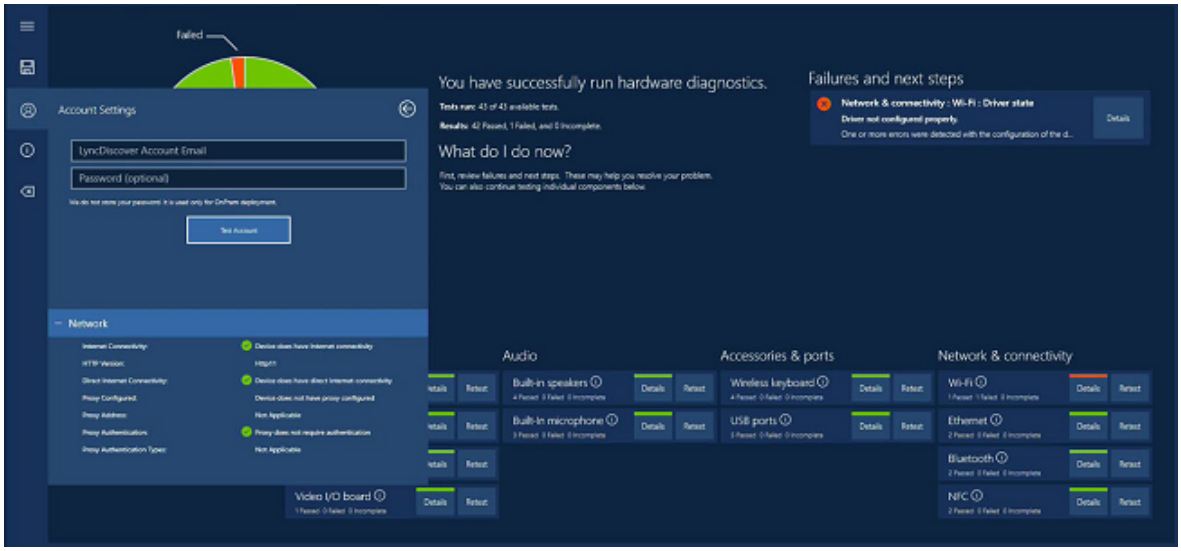
   

3. The next screen provides you the option to test all or some of the Surface Hub components. To begin testing the device account, select the **Test Results** icon.

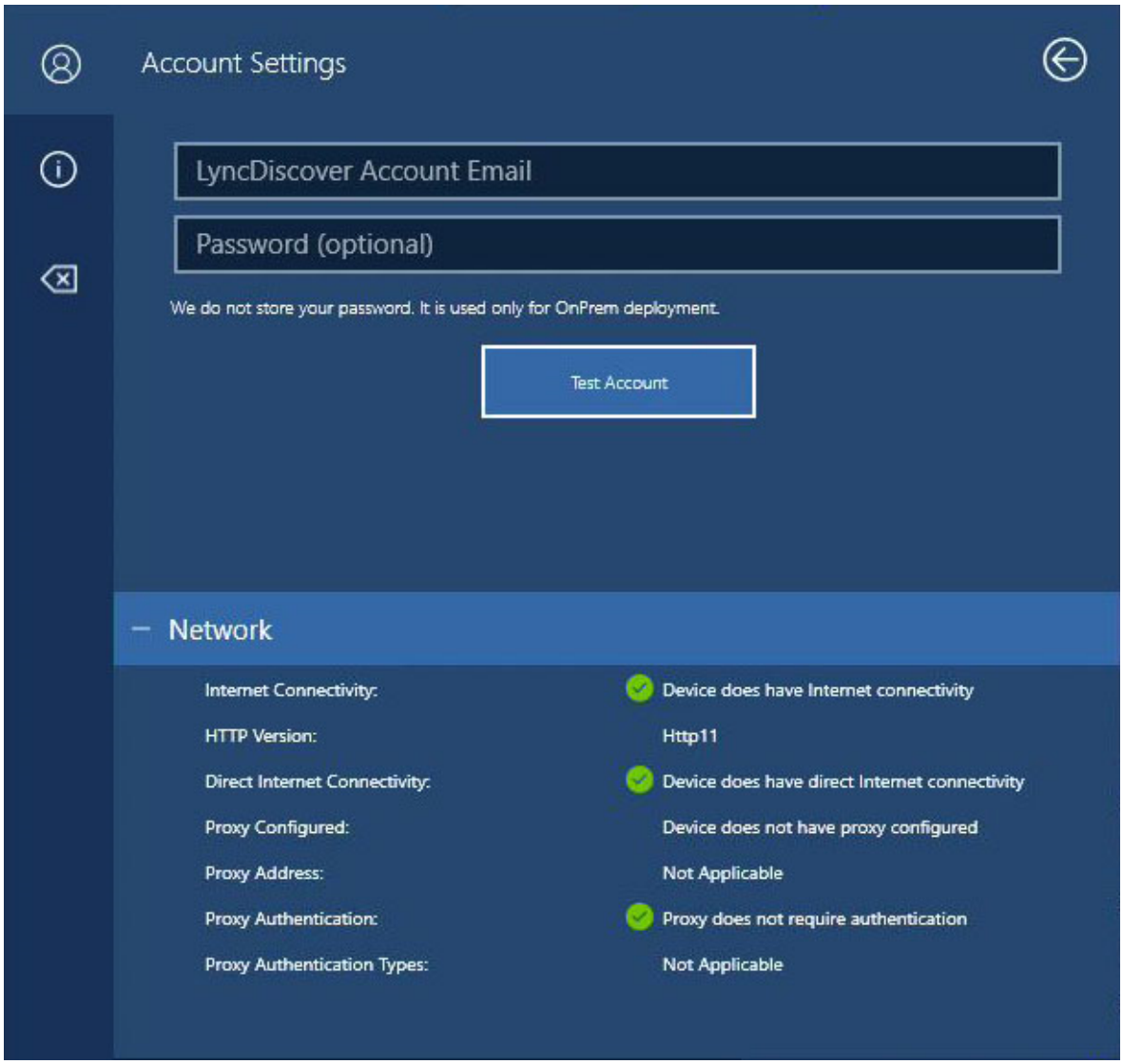




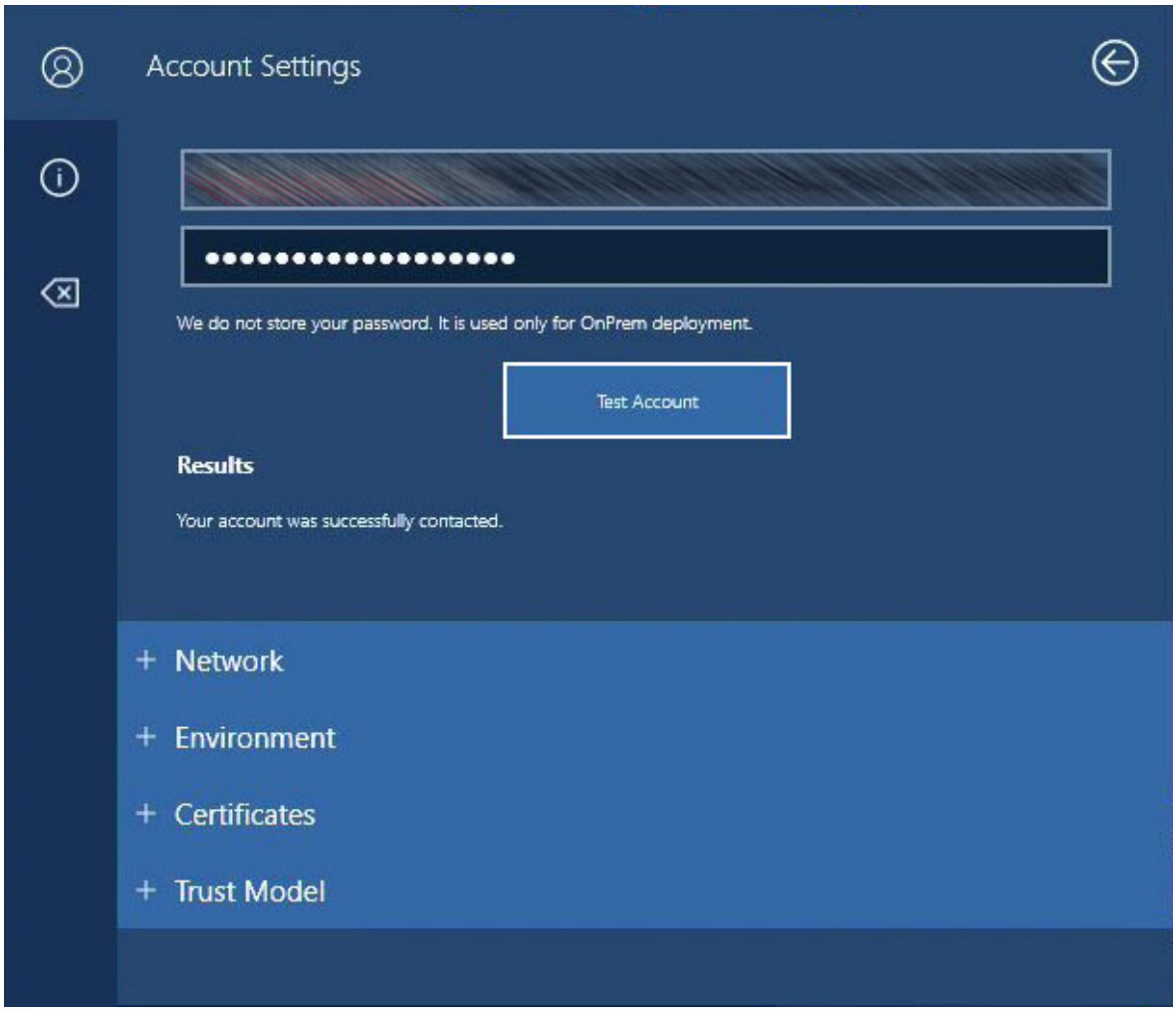
4. Select **Account Settings**.



The Account Settings screen is used to test your device account.

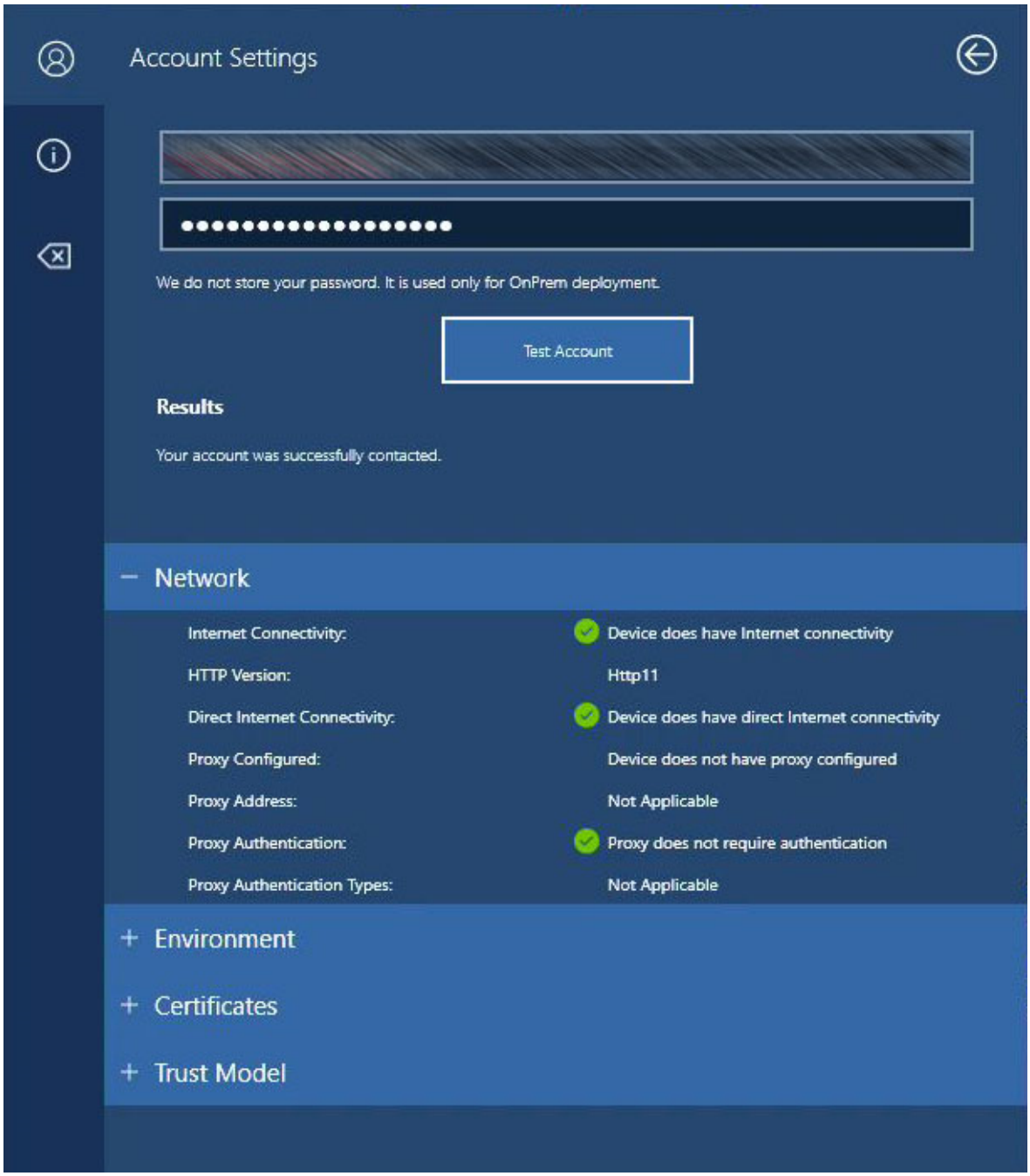


5. Enter the email address of your device account. The password is optional but is recommended. Select the **Test Account** button when you are ready to continue.

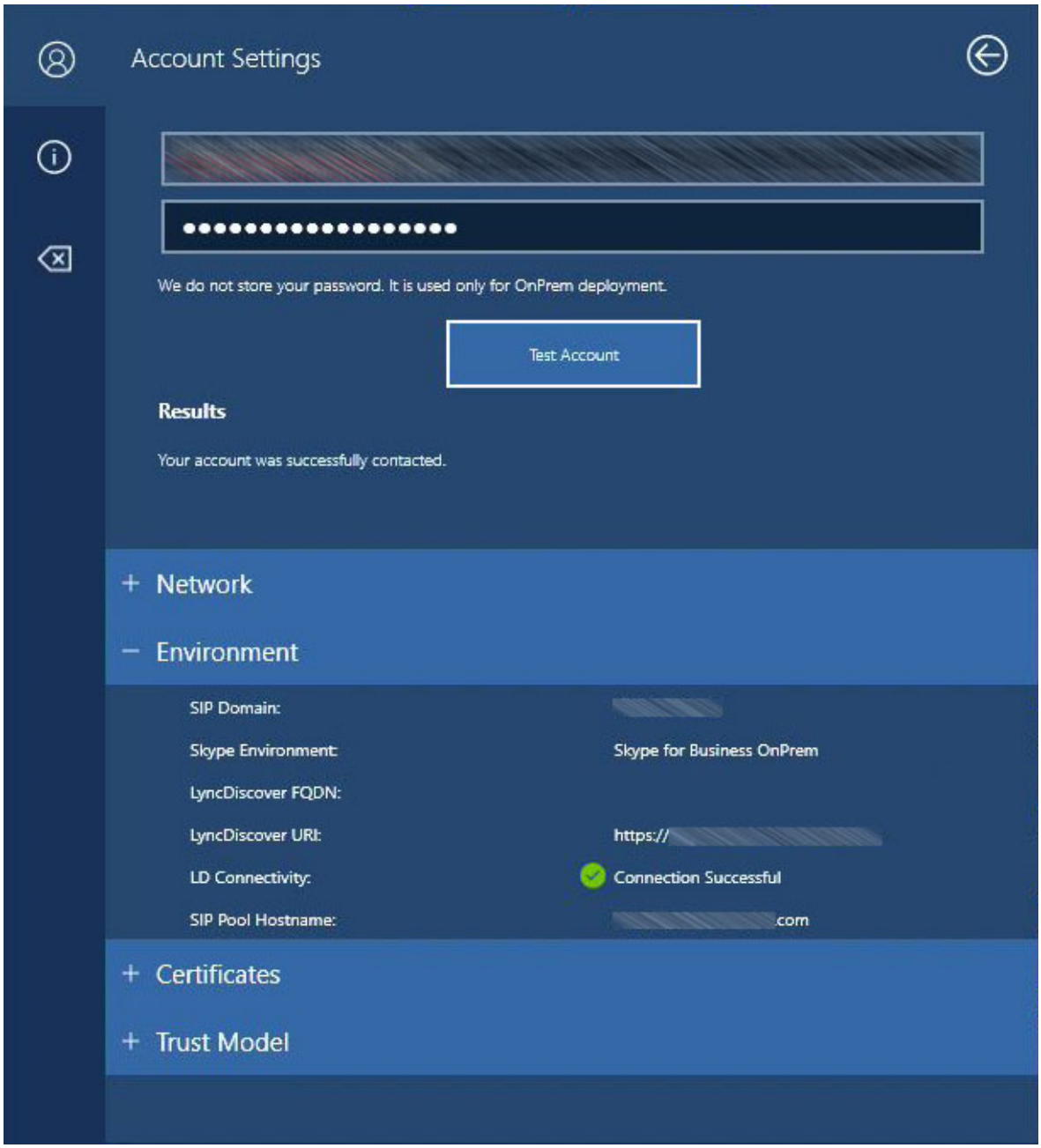


6. After testing is finished, review the results for the four areas of testing. Each section can be expanded or collapsed by selecting the Plus or Minus sign next to each topic.

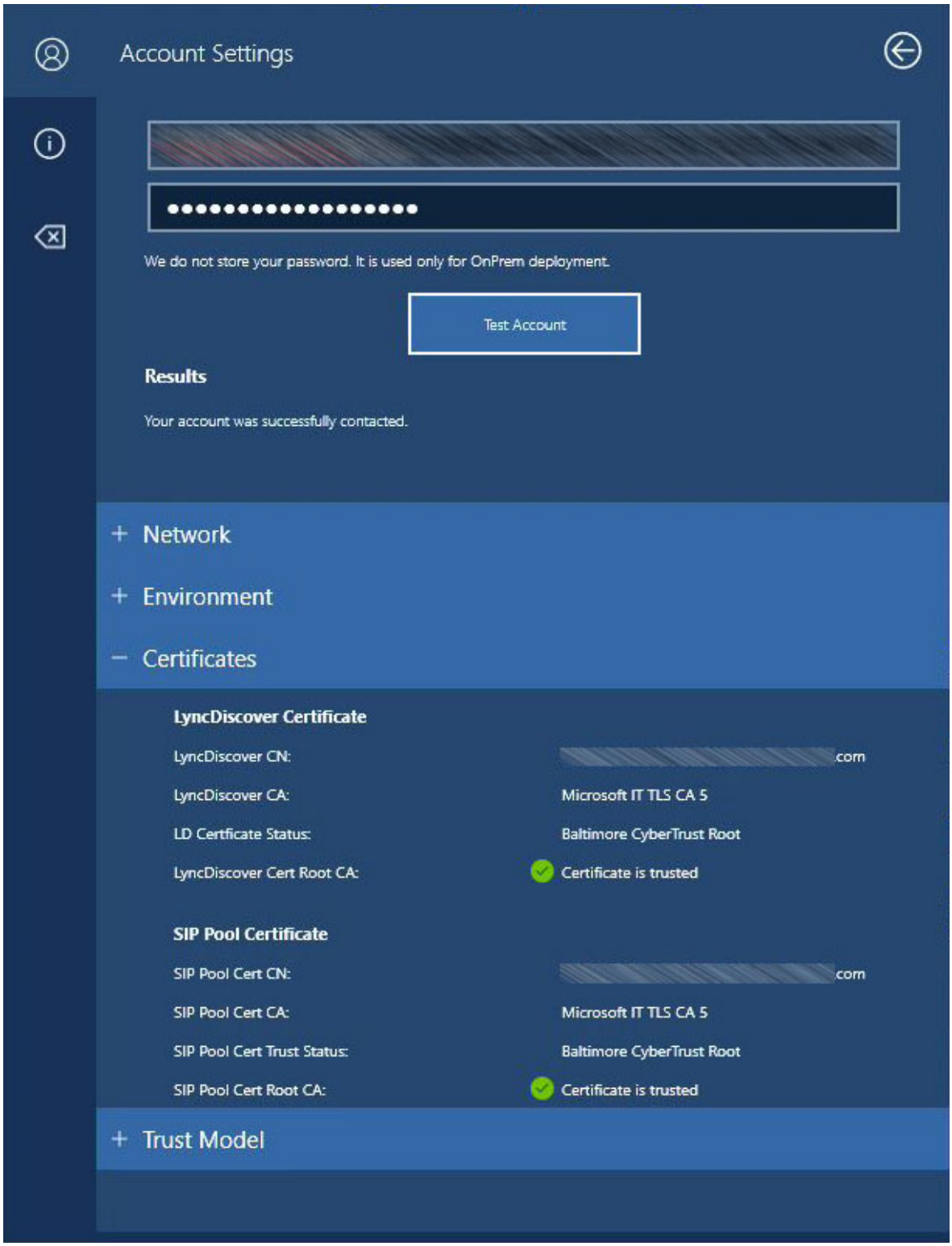
   Network



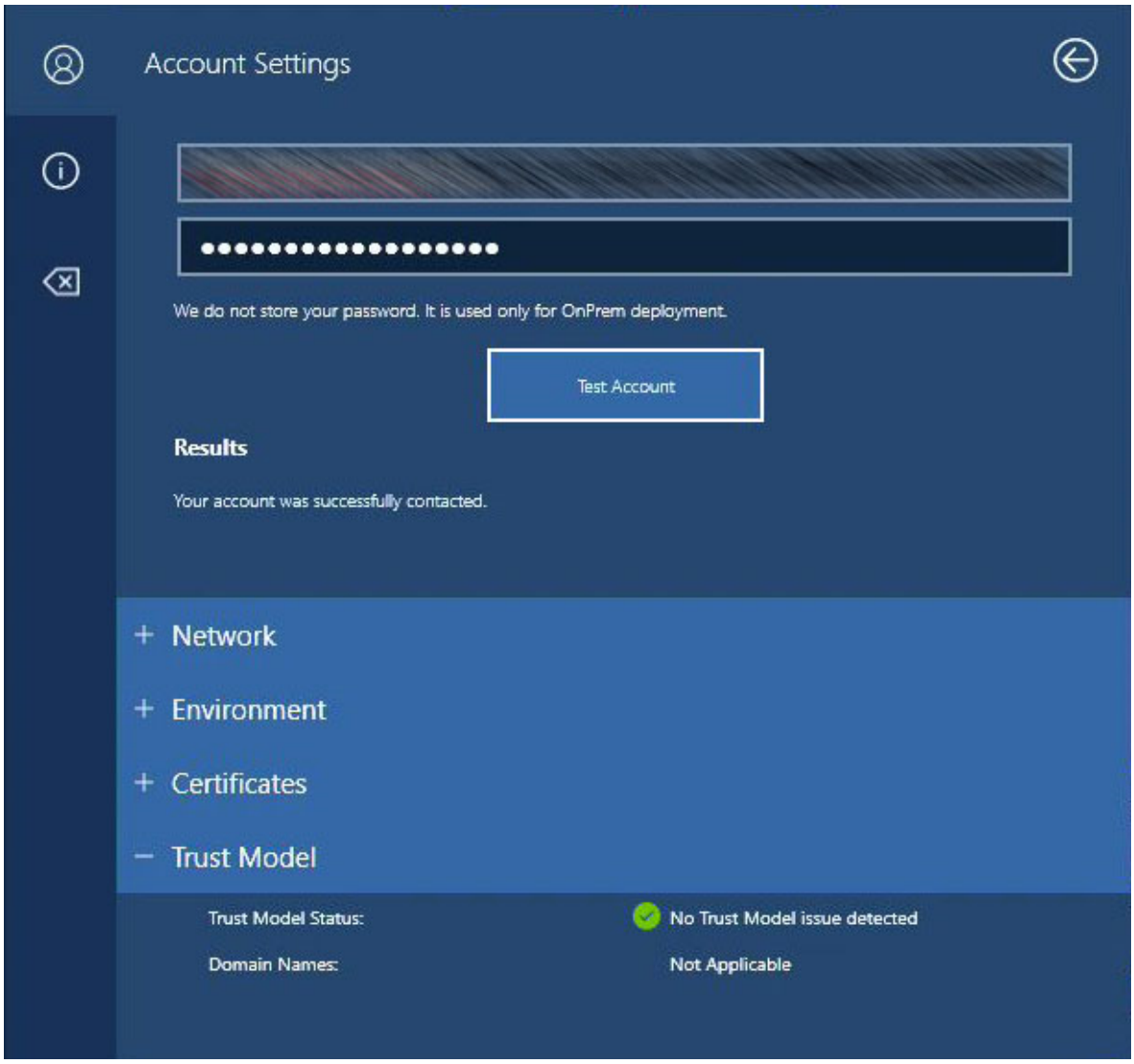
Environment



Certificates


Account Settings
We do not store your password. It is used only for OnPrem deployment.
Test Account
Results
Your account was successfully contacted.
Network
Environment
Certificates
LyncDiscover Certificate
LyncDiscover CN:
LyncDiscover CA:
Microsoft IT TLS CA 5
LD Certficate Status:
Baltimore CyberTrust Root
LyncDiscover Cert Root CA:
Certificate is trusted
SIP Pool Certificate
SIP Pool Cert CN:
SIP Pool Cert CA:
Microsoft IT TLS CA 5
SIP Pool Cert Trust Status:
Baltimore CyberTrust Root
SIP Pool Cert Root CA:
Certificate is trusted
Trust Model

Trust Model



Appendix

Field messages and resolution

Network

Field	Success	Failure	Comment	Reference
Internet Connectivity	Device does have Internet connectivity	Device does not have Internet connectivity	Verifies internet connectivity, including proxy connection	
HTTP Version	1.1	1.0	If HTTP 1.0 found, it will cause issue with WU and Store	

Field	Success	Failure	Comment	Reference
Direct Internet Connectivity	Device has a Proxy configured Device has no Proxy configured	N/A	Informational. Is your device behind a proxy?	
Proxy Address			If configured, returns proxy address.	
Proxy Authentication	Proxy does not require Authentication	Proxy requires Proxy Auth	Result may be a false positive if a user already has an open session in Edge and has authenticated through the proxy.	
Proxy Auth Types			If proxy authentication is used, return the Authentication methods advertised by the proxy.	

Environment

Field	Success	Failure	Comment	Reference
SIP Domain			Informational.	
Skype Environment	Skype for Business Online, Skype for Business OnPrem, Skype for Business Hybrid	Informational.	What type of environment was detected. Note: Hybrid can only be detected if the password is entered.	
LyncDiscover FQDN			Informational. Displays the LyncDiscover DNS result	
LyncDiscover URI			Informational. Displays the URL used to perform a LyncDiscover on your environment.	
LyncDiscover	Connection Successful	Connection Failed	Response from LyncDiscover web service.	

Field	Success	Failure	Comment	Reference
SIP Pool Hostname			Informational. Display the SIP pool name discovered from LyncDiscover	

Certificates (in-premises hybrid only)

LyncDiscover Certificate

Field	Success	Failure	Comment	Reference
LyncDiscover Cert CN			Informational. Displays the LD cert Common name	
LyncDiscover Cert CA			Informational. Displays the LD Cert CA	
LyncDiscover Cert Root CA			Informational. Displays the LD Cert Root CA, if available.	
LD Trust Status	Certificate is Trusted.	Certificate is not trusted, please add the Root CA.	Verify the certificate against the local cert store. Returns positive if the machine trusts the certificate.	Download and deploy Skype for Business certificates using PowerShell /Supported items for Surface Hub provisioning packages

SIP Pool Certification

Field	Success	Failure	Comment	Reference
SIP Pool Cert CN			(CONTENTS)	
SIP Pool Cert CA			(CONTENTS)	
SIP Pool Trust Status	Certificate is Trusted.	Certificate is not trusted, please add the Root CA.	Verify the certificate against the local cert store and return a positive if the devices trusts the certificate.	

Field	Success	Failure	Comment	Reference
SIP Pool Cert Root CA			Information. Display the SIP Pool Cert Root CA, if available.	

Trust Model (on-premises hybrid only)

Field	Success	Failure	Comment	Reference
Trust Model Status	No Trust Model Issue Detected.	SIP Domain and server domain are different please add the following domains.	Check the LD FQDN/ LD Server Name/ Pool Server name for Trust model issue.	
Domain Name(s)			Return the list of domains that should be added for SFB to connect.	

Find Teams Rooms devices with unsupported licenses

Article • 06/21/2023

Resource accounts that only have user licenses or Microsoft Teams Shared Device licenses assigned to them aren't supported for use with Microsoft Teams Rooms devices. Resource accounts used with Teams Rooms devices need to be assigned one of the following licenses:

- Microsoft Teams Rooms Pro
- Microsoft Teams Rooms Basic
- Microsoft Teams Rooms Standard (legacy)
- Microsoft Teams Rooms Premium (legacy)

> **ⓘ Important**
>
> User licenses aren't supported for use with meeting devices. User licenses that have been assigned to teams meeting devices need to be replaced by an approved Teams Rooms license prior to July 1, 2023. Meeting devices that do not have a Team Rooms license after July 1, 2023 will be granted a 90-day grace period ending on September 30, 2023. After the 90-day grace period, devices will be blocked from signing in until a Teams Rooms license is assigned.
>
> Also, **Microsoft Teams Shared Devices** licenses aren't supported on and won't work with Teams Rooms devices. Teams Rooms devices should only be assigned Teams Rooms Basic or Teams Rooms Pro licenses.

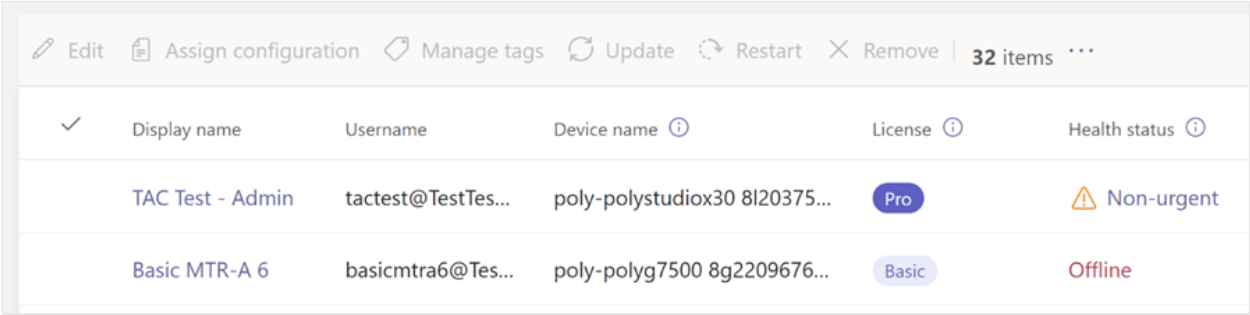
You have a couple of options for checking whether the resource accounts signed into your Teams Rooms devices have a Teams Rooms license. If you only have a couple Teams Rooms devices, use the steps in Check the license of a few Teams Rooms devices. If you have more than a few Teams Rooms devices, use the steps in Check the license of multiple Microsoft Teams Rooms devices.

For information about Teams Rooms licensing, see Microsoft Teams Rooms licenses.

Check the license of a couple Teams Rooms devices

For a small number of devices, you can see what license your devices have by going to Teams devices in the Teams admin center, and then selecting the device category (**Teams Rooms on Windows**, **Teams Rooms on Android**, or **Surface Hubs**) you want to see.

For example, if you select **Teams devices** > **Teams Rooms on Windows**, you'll see the following image. The **License** column shows the Teams Rooms license assigned to each device.



Devices that have the Teams Rooms Pro license can access all the capabilities of their Teams Rooms devices. Devices with other Teams Rooms licenses can access a subset of those features. You can see which features are available to each license in Teams Rooms Basic and Teams Rooms Pro feature comparison.

Check the license of multiple Microsoft Teams Rooms devices

Checking licenses for Teams Rooms devices one at a time can be time consuming. To make this process easier, we're making available a sample script that checks the licenses of all your Teams Rooms devices. The script provides you with a list of the resource accounts that are associated with your Teams Rooms devices, organized by license type. Resource accounts with licenses that aren't supported with Teams Rooms devices are grouped together for your review. If resource accounts associated with Teams Rooms devices have an unsupported license type, you'll need to change it to a supported license before July 1, 2023.

Take a look at this short video to see how to use the example script to audit your licenses:
https://www.youtube-nocookie.com/embed/Jd_dT4beJDw

PowerShell

```
<#PSScriptInfo
.VERSION 0.25
```

```
.GUID

.AUTHOR Peter Lurie, Mark Hodge

.COMPANYNAME Microsoft

.COPYRIGHT (c) 2022-2023 Peter Lurie & Mark Hodge

.TAGS Microsoft Teams Room System Surface Hub MEETING_ROOM for Resource
Accounts

.LICENSEURI   https://creativecommons.org/licenses/by/4.0/?ref=chooser-v1

.PROJECTURI

.ICONURI

.EXTERNALMODULEDEPENDENCIES

.REQUIREDSCRIPTS

.EXTERNALSCRIPTDEPENDENCIES

.RELEASENOTES

Version 0.23:  Updated to improve support for CSV output

Version 0.24:  updating file/path UI

Version 0.25:  udpated to to filter on the server vs. local per feedback

#>



<#

.SYNOPSIS

Reports out the list of resource accounts that have assigned licenses,
highlighting the ones with Teams Meeting Room liceses in green

.DESCRIPTION

This script uses Graph Powershell & EXO to check for resource accounts and
their licenses.

.PARAMETER

None

.NOTES

author: Peter Lurie
```

```
created: 2022-05-10

editied: 2023-05-30

#>



Function Get-SaveFilePath ([string]$initialDirectory) {  #prompts for
filename and path for exporting to CSV, if needed



      Add-Type -AssemblyName System.Windows.Forms

      $SaveFileDialog = New-Object System.Windows.Forms.SaveFileDialog

      $SaveInitialPath = ".\"

      $SaveFileName = "TeamsMeetingRoomLicenses.csv"

    $SaveFileDialog.initialDirectory = $SaveInitialPath #Sets current
starting path

    $SaveFileDialog.filter = "CSV (*.csv)| *.csv"    #Restricts to CSV by
default

      $SaveFileDialog.FileName = $SaveFileName                    #Default
filename



 $SaveFileDialog.ShowDialog()   #actually asks for the filepath

      return $SaveFileDialog.filename #Returns filepath for writing to CSV

}



Clear-Host

Write-Host

Write-Host "Welcome to Meeting Room License Checker." -ForegroundColor Green

Write-Host

Write-Host "This tool will look through your Exchange Online and AAD to find
Resource Account Mailbox UPNs."

Write-host "It will then report which resource accounts have Teams Room
licenses, which have no license, and which have some other licenses"

Write-host "This is ver 0.25."
```

```
Write-Host




#Setup for Graph

Write-Host "Loading Microsoft Graph Modules"

If (!(Get-Module -listavailable | Where-Object {$_.name -like
"*Microsoft.Graph.Users*"}))

      {

             Install-Module Microsoft.Graph.Users  #-ErrorAction
SilentlyContinue

      }

Else

      {     Import-Module Microsoft.Graph.Users  #-ErrorAction
SilentlyContinue

      }

Try

      {     write-host "Getting ready to connect to the Microsoft Graph"

        Connect-MgGraph -Scopes "User.Read.All"

             write-host "Connected successfully the Microsoft Graph" -
ForegroundColor Green

      }

Catch

      {     write-host "Unable to connect to your Microsoft Graph
Environment" -ForegroundColor Red

      }



Write-Host

Write-Host "Getting ready to connect to Exchange Online." -ForegroundColor
Green

If (!(Get-Module -listavailable | Where-Object {$_.name -like
"*ExchangeOnlineManagement*"}))
```

```
      {     Install-Module ExchangeOnlineManagement  -ErrorAction
SilentlyContinue

      }

Else

      {     Import-Module ExchangeOnlineManagement  -ErrorAction
SilentlyContinue

      }

Try

      {     write-host "Connecting to your Exchange Online instance"

        Connect-ExchangeOnline  -ShowBanner:$false #Note if using GCC, DOD,
or a soverign cloud, see docs for this command for the correct -
ExchangeEnvironmentName.  Default is Commerical cloud

             write-host "Connected successfully to your Exchange Online"  -
ForegroundColor Green

      }

Catch

      {     write-host "Unable to connect to your Exchange Online
Environment"  -ForegroundColor Red

      }



Write-Host

Write-Host "Starting to search for Resource Account Mailbox UPNs and their
licenses..." -ForegroundColor Green

$StartElapsedTime = $(get-date)

[System.Collections.ArrayList]$No_License = @()

[System.Collections.ArrayList]$MTR_Premium_License = @()    # Also includes
MMR1 license

[System.Collections.ArrayList]$MeetingRoom_License = @()   #Teams Meeting
Room Standard license

[System.Collections.ArrayList]$MeetingRoomPro_License = @()  #Optimal
license

[System.Collections.ArrayList]$MeetingRoomBasic_License = @()  #Basic
license does max out at 25 licenses/tenant
```

```
[System.Collections.ArrayList]$MeetingRoomOther_License = @()  #Licenses
OTHER than what should be applied to a Teams Room Resource Account

$Report = [System.Collections.Generic.List[Object]]::new()



#Updated to filter server side and not client side.  See next line for new
filter.

#$Room_UPNs = get-mailbox | Where-Object {$_.recipientTypeDetails -eq
"roomMailbox"} | Select-Object DisplayName, PrimarySmtpAddress,
ExternalDirectoryObjectId



$Room_UPNs = Get-ExoMailbox -Filter {recipientTypeDetails -eq "RoomMailbox"
} | Select-Object DisplayName, PrimarySmtpAddress, ExternalDirectoryObjectId

Write-Host $Room_UPNs.Length " were found." -ForegroundColor Green

Write-Host "Note that resource accounts can contain 0 or multiple licenses.
As such, the total of all licenses discovered may be different than the
number of resource accounts" -ForegroundColor Yellow

Write-Host



$i,$x = 0,$Room_UPNs.count   #Setup for counting devices

if ($null -eq $x) {$x = 1}   #run through the loop at least once to print
results, otherwise will get a divide/0 error

# Note that resource accounts can contain multiple licenese.  As such, the
sum of all licenses may exceed the number of resource accounts



ForEach ($UPN in $Room_UPNs){

    $i++

      Write-Progress -activity "Searching for resource accounts with
licenses..." -status "Scanned: $i of $x"

    $UPN_license =  Get-MgUserLicenseDetail -UserID
$UPN.ExternalDirectoryObjectId | Select-Object -ExpandProperty SkuPartNumber

    $temp =
[pscustomobject]@{'DisplayName'=$UPN.DisplayName;'UPN'=$UPN.PrimarySmtpAddre
ss; 'Licenses'=$UPN_license -join ", "} #pulls out the license from a UPN
```

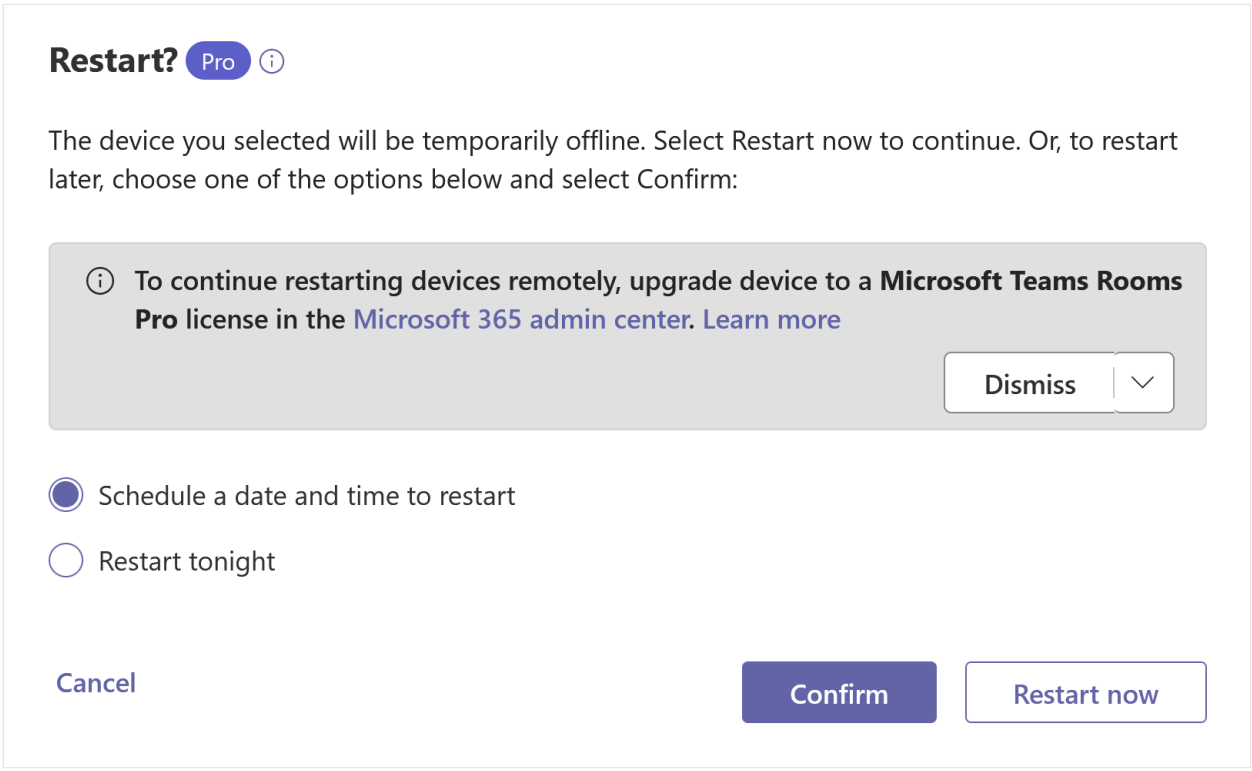
```
    if ($null -eq $UPN_license) {$No_License.add($temp) | Out-Null}  #find
resource accounts without licenses



      if ($UPN_license -like "MTR_PREM*" -or $UPN_license -like "MMR_P*" )
{$MTR_Premium_License.add($temp) | Out-Null}   #find resource accounts with
legacy MTR Premium

    if ($UPN_license -like "MEETING_ROOM*") {$MeetingRoom_License.add($temp)
| Out-Null}   #find resource accounts with legacy Teams Room Standard
licenses

    if ($UPN_license -like "Microsoft_Teams_Rooms_Pro*")
{$MeetingRoomPro_License.add($temp) | Out-Null}   #find resource accounts
with meeting room pro licenses

      if ($UPN_license -like "Microsoft_Teams_Rooms_Basic*")
{$MeetingRoomBasic_License.add($temp) | Out-Null}   #find resource accounts
with meeting room basic licenses



    if (!(($UPN_license -like "MEETING_ROOM*" ) -or ($UPN_license -like
"Microsoft_Teams_Rooms_*" ) -or ($UPN_License -like "MTR_PREM") -or
($UPN_License -like "MMR_P1")-or ($null -eq $UPN_license) ))
{$MeetingRoomOther_License.add($temp) | Out-Null}  #If there are resource
accounts that have other licenses, add them too.



    $Report.Add($temp)   #Creating the file for the CSV, if needed later



    $temp = $null

      }







    Write-Progress -Completed -activity "Searching for resource accounts
with licenses..."



Write-Host
```

```
Write-Host $No_License.count "Resource accounts without any licenses.
(Typically these would be bookable rooms without any Teams Meeting
technology or resource accounts yet to be licensed.)" -ForegroundColor Cyan

$No_License | Sort-Object UPN | Format-Table

Write-Host

Write-Host

Write-Host $MeetingRoom_License.count "resource accounts with Legacy Teams
Room Standard licenses. (Typically, these licenses should be upgraded to
Teams Room Pro at EA Renewal)." -ForegroundColor Yellow

$MeetingRoom_License | Sort-Object UPN | Format-Table

Write-Host

Write-Host

Write-Host $MTR_Premium.count "Resource accounts with Teams Room Premium or
MMR license. (Typically, these licenses should be migrated to Teams Room Pro
at EA Anniversary/Renewal)." -ForegroundColor Red

$MTR_Premium | Sort-Object UPN | Format-Table

Write-Host

Write-Host

Write-Host $MeetingRoomPro_License.count "Resource accounts with MTR Pro
licenses." -ForegroundColor Green

$MeetingRoomPro_License | Sort-Object UPN | Format-Table

Write-Host

Write-Host

Write-Host $MeetingRoomBasic_License.count "Resource accounts with Teams
Room System Basic licenses." -ForegroundColor Green

$MeetingRoomBasic_License | Sort-Object UPN | Format-Table

Write-Host

Write-Host

Write-Host $MeetingRoomOther_License.count "Resource accounts with licenses
other than Teams Room System licenses. (Confirm if these licenses are
actually needed)." -ForegroundColor Yellow

$MeetingRoomOther_License | Sort-Object UPN | Format-Table

Write-Host
```

```
Write-Host



$elapsedTime = $(get-date) - $StartElapsedTime

$totalTime = "{0:HH:mm:ss}" -f ([datetime]$elapsedTime.Ticks)

Write-Host "Processing took $totalTime."  -ForegroundColor Green

Write-Host

Write-Host

$answer = read-host -prompt "Do you want to export results to a CSV file?
[y/N]"

If ($answer.ToLower() -eq 'y' )

      {

            try {

                  $SaveMyFile = Get-SaveFilePath    #Use Get-SaveFilePath
function to prompt for filepath information

                  $Report |  Sort-Object  UPN  | Export-CSV -Path
$SaveMyFile[1] -NoTypeInformation

                  Write-Host "Results Saved." -ForegroundColor green

            }

            catch {

                  Write-Host "Unable to save CSV" -ForegroundColor red

                  }

      }



Write-Host

Write-host "Note: MgGraph and ExchangeOnline connections were not
disconnected.  Use Disconnect-ExchangeOnline and Disconnect-MgGraph if
needed."  -ForegroundColor yellow

Write-Host

Write-Host "Done" -ForegroundColor Green
```

See which features require a Microsoft Teams Rooms Pro license

Features that require a Microsoft Teams Rooms Pro license can be identified by looking for the icon on a device's details page. If the device that's currently selected isn't assigned a Microsoft Teams Rooms Pro license, you can't perform the action and a prompt to upgrade is displayed.



Related Content

- Step 1 - Purchase a license for the Teams Rooms console
- Teams add-on licensing
- Manage user access to Teams
- View licenses and services with PowerShell
- Product names and service plan identifiers for licensing
- Education SKU reference
- How long does it take for new license orders to appear in the license summary

Hybrid deployment on Surface Hub

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

In a hybrid deployment, your organization has a mix of services, with some hosted on premises and some hosted online through Microsoft 365 or Microsoft 365. With Microsoft Teams Rooms, the following hybrid scenarios are supported:

- Exchange Online with Skype for Business Server on premises. For more information, see Skype Room System hybrid deployments
- Exchange on-premises with Microsoft Teams (Skype online is no longer available). For more information, see Create and configure resource accounts for rooms and shared Teams devices.

Learn more

- Create and test a device account

Modern authentication on Surface Hub

Article • 01/03/2023 • Applies to: Surface Hub 2S 2020 Update

The Windows 10 Team 2020 Update adds support for modern authentication of the Hub device account in some scenarios. Once you install the 2020 update, you can migrate from legacy basic authentication to make use of the latest security improvements if the device account authenticates via Azure Active Directory and the account's mailbox is hosted in Exchange Online. With the 2020 Update, Surface Hub supports Exchange Web Services (EWS) protocols and OAuth-based authentication when syncing the device account with Exchange Online.

For new cloud-based accounts, the Surface Hub automatically uses Modern Authentication to connect to Exchange Online without requiring additional configuration beyond simply adding the device account to the Surface Hub using the format alias@contoso.com. Do not use the legacy format – Contoso\alias, which is not supported for modern authentication. For more information, see create and test a device account.

> **Note**
>
> Modern authentication is not supported for on-premises Surface Hub accounts. For full modern auth functionality, the accounts must use **cloud authentication in Azure AD**. If **federated authentication** is used, the account authentication with the federated identity provider will still use legacy protocols.

Enroll Surface Hub into MDM management

Article • 02/16/2023 • Applies to: Surface Hub 2S, Surface Hub

You can enroll Surface into Microsoft Intune or other MDM provider via manual or auto enrollment.

Manual enrollment

1. Open the **Settings** app and sign in as a local administrator. Select **Surface Hub** > **Device management** and then select **+Device management**.
2. You will be prompted to sign in with the account to use for your MDM provider. After authenticating, the device automatically enrolls with your MDM provider.

> **Tip**
>
> If you're using Intune and the server address is not detected, enter **manage.microsoft.com**.

> **Note**
>
> MDM enrollment uses the account details provided for authentication. The account must have permissions to enroll a Windows device as well as an Intune license (or the equivalent enrollment promissions configured in your third-party MDM provider).

Auto Enrollment — Azure AD affiliated

During the initial setup process, when affiliating Surface Hub with an Azure Active Directory (AD) tenant that has Intune auto enrollment enabled, the device will automatically enroll with Intune. To learn more, refer to Intune enrollment methods for Windows devices. Azure AD affiliation and Intune auto enrollment are required for the Surface Hub to be a "compliant device" in Intune.

Manage Surface Hub via MDM

- See Manage Surface Hub with an MDM provider

Configure non-Global Admin accounts on Surface Hub

Article • 04/19/2023 • Applies to: Surface Hub, Surface Hub 2S

The Windows 10 Team 2020 Update adds support for configuring non-Global Admin accounts that limit permissions to management of the Settings app on Surface Hub devices joined to an Azure AD domain. This enables you to scope admin permissions for Surface Hub only and prevent potentially unwanted admin access across an entire Azure AD domain.

Windows 10 Team 2020 Update 2 adds support for LocalUsersAndGroups CSP. That is now the recommended CSP to use; RestrictedGroups CSP is still supported, but has been deprecated.

> **Note**
>
> Before you begin, make sure your Surface Hub is Azure AD-joined and Intune auto-enrolled. If not, you will need to **reset the Surface Hub** and complete the **first-time, out-of-the-box (OOBE) setup** again, choosing the option to join Azure AD. Only accounts that **authenticate via Azure AD** are supported with the non-Global Admin policy configuration.

Summary

The process of creating non-Global Admin accounts involves the following steps:

1. In Microsoft Intune, create a Security group containing the admins designated to manage Surface Hub.
2. Obtain Azure AD Group SID using PowerShell.
3. Create an XML file containing Azure AD Group SID.
4. Create a Security Group containing the Surface Hub devices that the non-Global admins Security group will manage.
5. Create a custom Configuration profile targeting the security group that contains your Surface Hub devices.

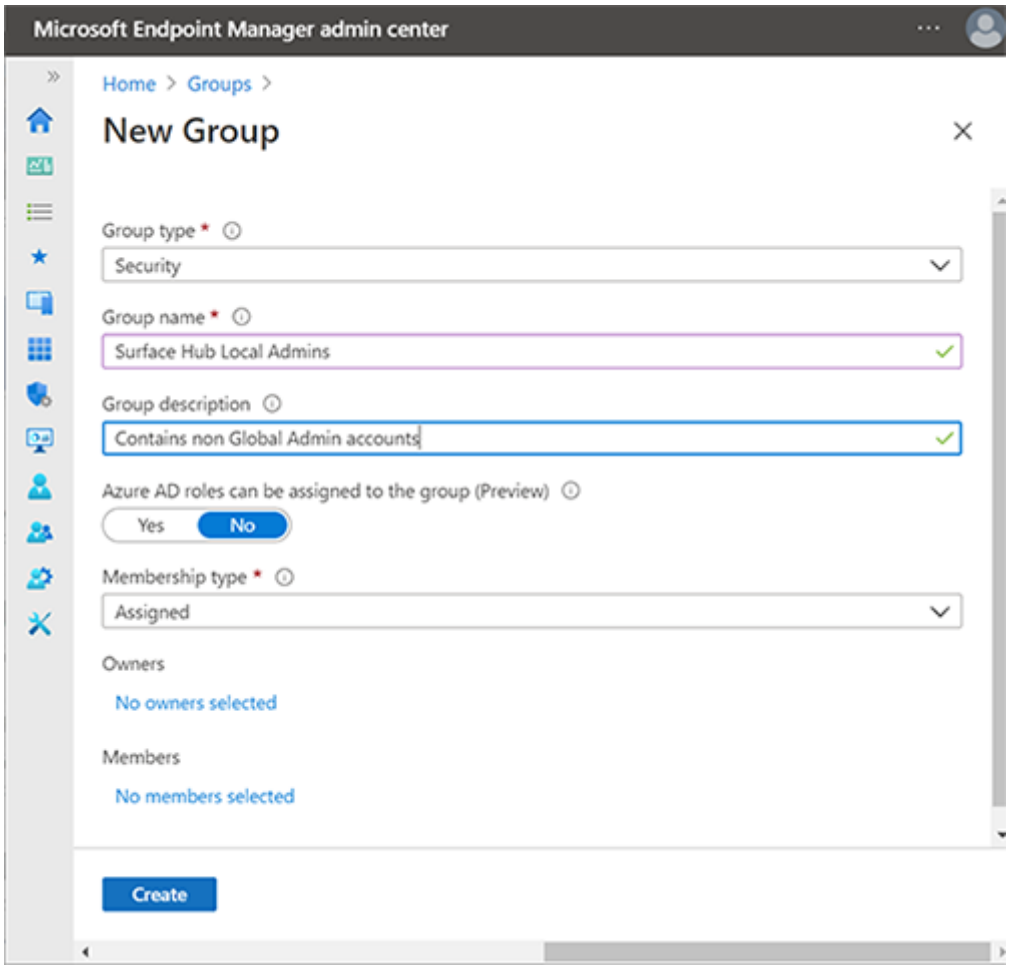
Create Azure AD security groups

First, create a security group containing the admin accounts. Then create another security group for Surface Hub devices.

Create security group for Admin accounts

1. Sign in to Intune via the Microsoft Intune admin center, select **Groups** > **New Group** > and under Group type, select **Security.**

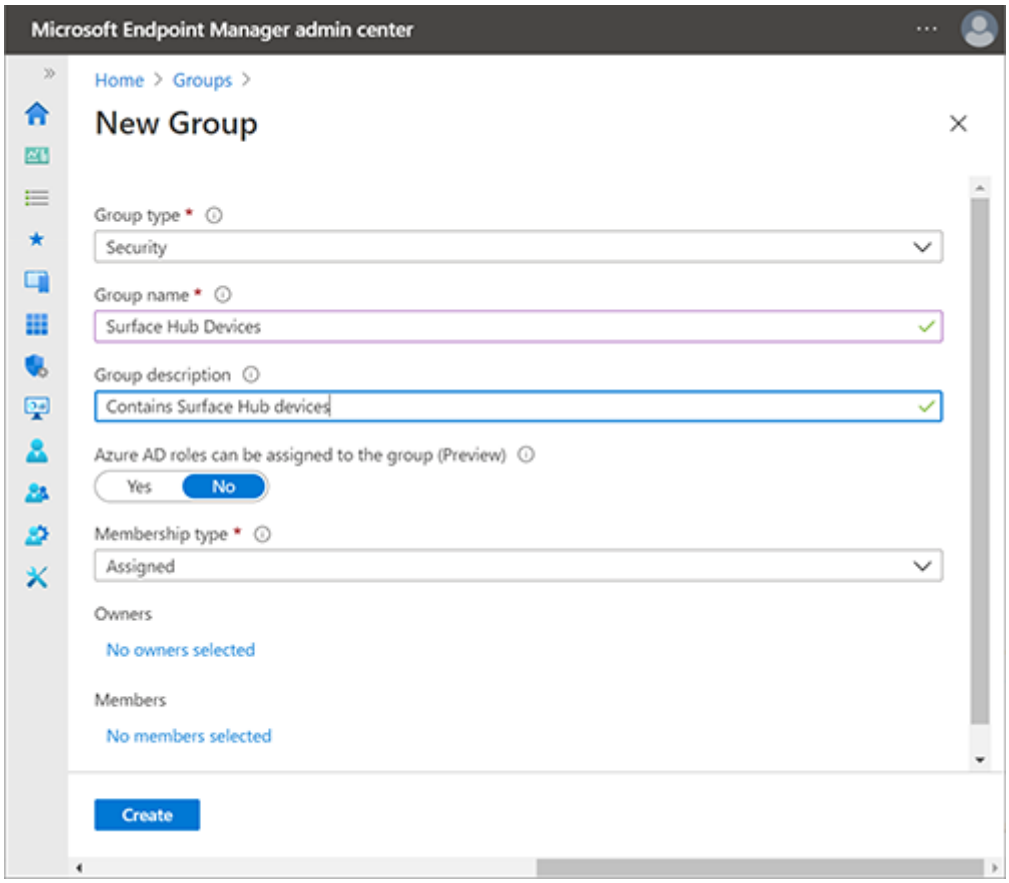
2. Enter a Group name -- for example, **Surface Hub Local Admins** -- and then select **Create.**



3. Open the group, select **Members**, and choose **Add members** to enter the Administrator accounts you wish to designate as non-Global admins on Surface Hub. To learn more about creating groups in Intune, see Add groups to organize users and devices.

Create security group for Surface Hub devices

1. Repeat the previous procedure to create a separate security group for Hub devices; for example, **Surface Hub devices**.



Obtain Azure AD Group SID using PowerShell

1. Launch PowerShell with elevated account privileges (**Run as Administrator**) and ensure your system is configured to run PowerShell scripts. To learn more, refer to About Execution Policies.

2. Install Azure PowerShell module.

3. Sign in to your Azure AD tenant.

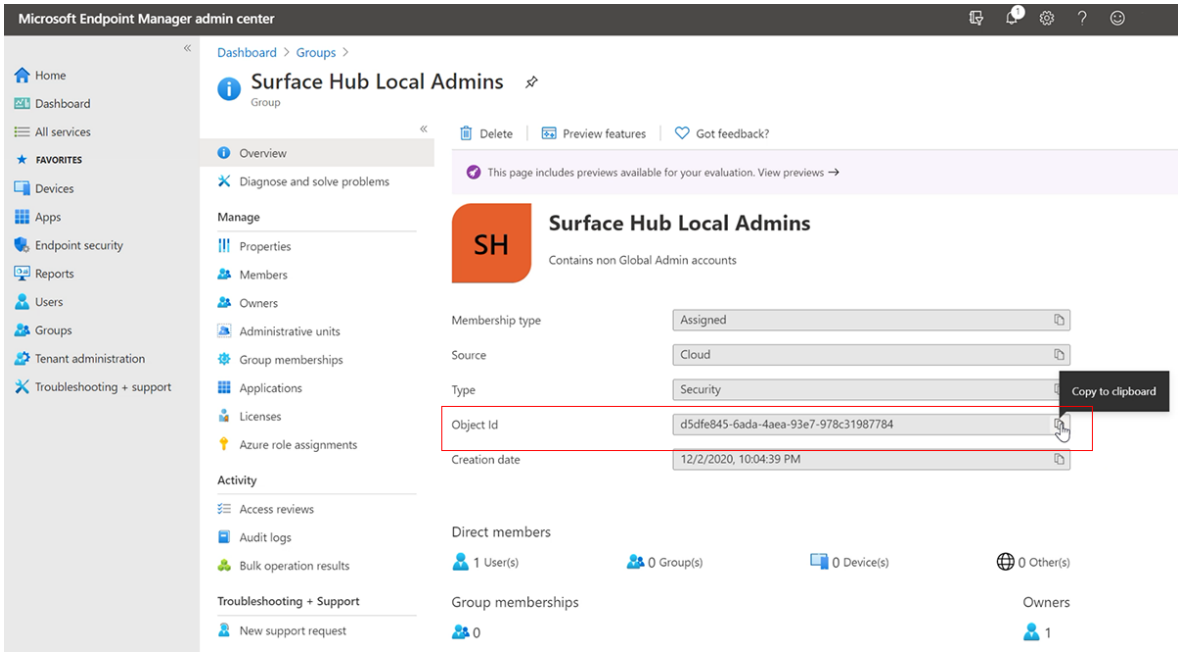
```PowerShell
Connect-AzureAD
```

4. When you're signed in to your tenant, run the following commandlet. It will prompt you to "Please type the Object ID of your Azure AD Group."

```PowerShell
function Convert-ObjectIdToSid
{    param([String] $ObjectId)
     $d=[UInt32[]]::new(4);
[Buffer]::BlockCopy([Guid]::Parse($ObjectId).ToByteArray(),0,$d,0,16);"
S-1-12-1-$d".Replace(' ','-')
```

```
}
```

5. In Intune, select the group you created earlier and copy the Object id, as shown in the following figure.



6. Run the following commandlet to get the security group's SID:

PowerShell

```
$AADGroup = Read-Host "Please type the Object ID of your Azure AD
Group"
$Result = Convert-ObjectIdToSid $AADGroup
Write-Host "Your Azure Ad Group SID is" -ForegroundColor Yellow $Result
```

7. Paste the Object id into the PowerShell commandlet, press **Enter**, and copy the **Azure AD Group SID** into a text editor.

Create XML file containing Azure AD Group SID

1. Copy the following into a text editor:

XML

```
<GroupConfiguration>
<accessgroup desc = "S-1-5-32-544">
    <group action = "U" />
    <add member = "AzureAD\bob@contoso.com"/>
    <add member = "S-1-12-1-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-
XXXXXXXXXX"/>
```

```
</accessgroup>
</GroupConfiguration>
```

2. Replace the placeholder SID (beginning with S-1-12-1) with your **Azure AD Group SID** and then save the file as XML; for example, **aad-local-admin.xml**.

> ⓘ **Note**
>
> While groups should be specified via their SID, if you would like to add Azure users directly, specify their User Principal Names (UPNs) in this format: `<member name = "AzureAD\user@contoso.com" />`

Create Custom configuration profile

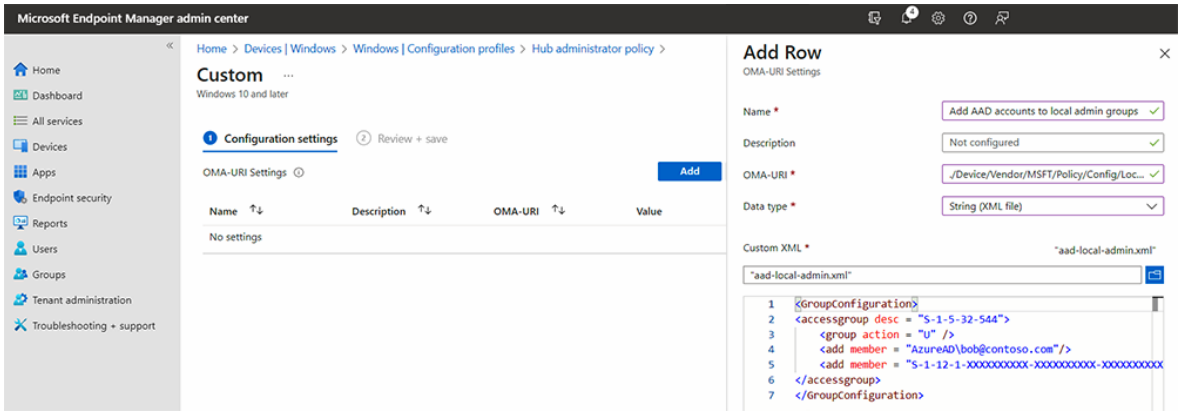
1. In Endpoint Manager, select **Devices** > **Configuration profiles** > **Create profile**.
2. Under Platform select **Windows 10 and later.** Under Profile, select **Templates** > **Custom** > **Create.**
3. Add a name and description and then select **Next.**
4. Under **Configuration settings** > **OMA-URI Settings**, select **Add**.
5. In the Add Row pane, add a name and under **OMA-URI**, add the following string:

```
OMA-URI
```

```
./Device/Vendor/MSFT/Policy/Config/LocalUsersAndGroups/Configure
```

> ⓘ **Note**
>
> The **RestrictedGroups/ConfigureGroupMembership** policy setting also allows you to configure members (users or AAD groups) to a Windows 10 local group. However, it only allows for a complete replacement of the existing groups with the new members. You cannot selectively add or remove members. Available in Windows 10 Team 2020 Update 2, it is recommended to use the **LocalUsersandGroups** policy setting instead of the RestrictedGroups policy setting. Applying both policy settings to Surface Hub is unsupported and may yield unpredictable results.

6. Under Data type, select **String XML** and browse to open the XML file you created in the previous step.



7. Click **Save**.

8. Click **Select groups to include** and choose the security group you created earlier (**Surface Hub devices**). Click **Next.**

9. Under Applicability rules, add a Rule if desired. Otherwise, select **Next** and then select **Create**.

To learn more about custom configuration profiles using OMA-URI strings, see Use custom settings for Windows 10 devices in Intune.

Non Global admins managing Surface Hub

Members of the newly configured **Surface Hub Local Admins** Security group can now sign in to the Settings app on Surface Hub and manage settings.

> **Important**
>
> Unless the Update ("U") action of the **LocalUsersAndGroups CSP** is the only configuration used, the pre-existing access of global admins to the Settings app is removed.

Create provisioning packages for Surface Hub

Article • 04/05/2023 • Applies to: Surface Hub, Surface Hub 2S

Provisioning packages allow you to automate deployment of key features, helping deliver a consistent experience across all Surface Hubs in your organization. Using Windows Configuration Designer (WCD) on a separate PC, you can complete the following tasks:

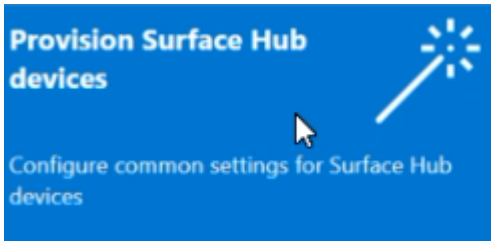
- Enroll in Active Directory or Azure Active Directory
- Create a device administrator account
- Add applications and certificates
- Configure proxy settings
- Configure Configuration Service Provider (CSP) settings

Overview

1. On a separate PC running Windows 10 or Windows 11, install Windows Configuration Designer from the Microsoft Store.
2. Select **Provision Surface Hub devices** to configure common settings using a wizard. Or select Advanced provisioning to view and configure all possible settings.
3. Create the provisioning package and save it to a USB drive.
4. Deploy the package to your Surface Hub during first-run setup, or through the Settings app. To learn more, see Create a provisioning package.

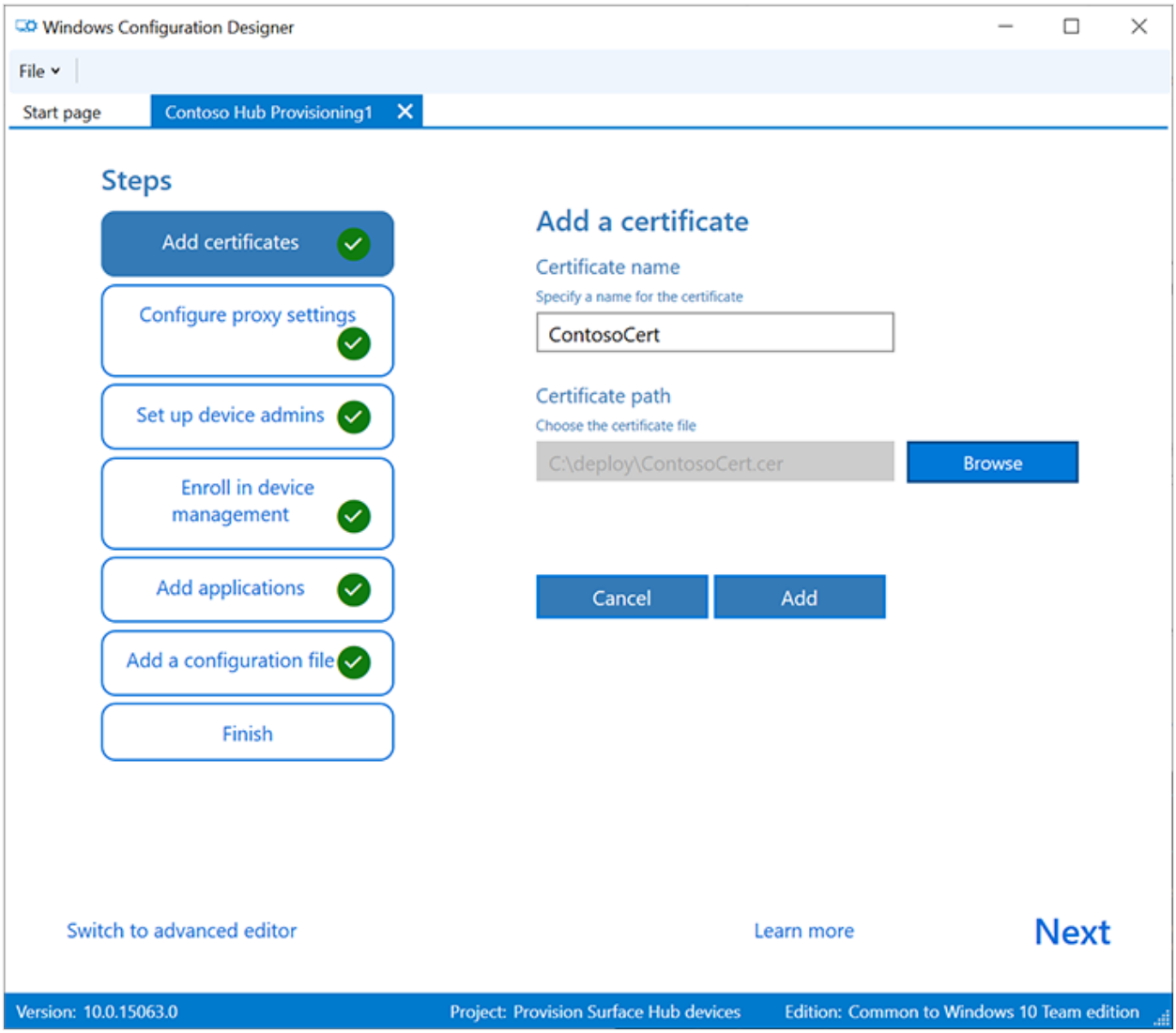
Use Surface Hub provisioning wizard

1. Open Windows Configuration Designer and select **Provision Surface Hub devices**.



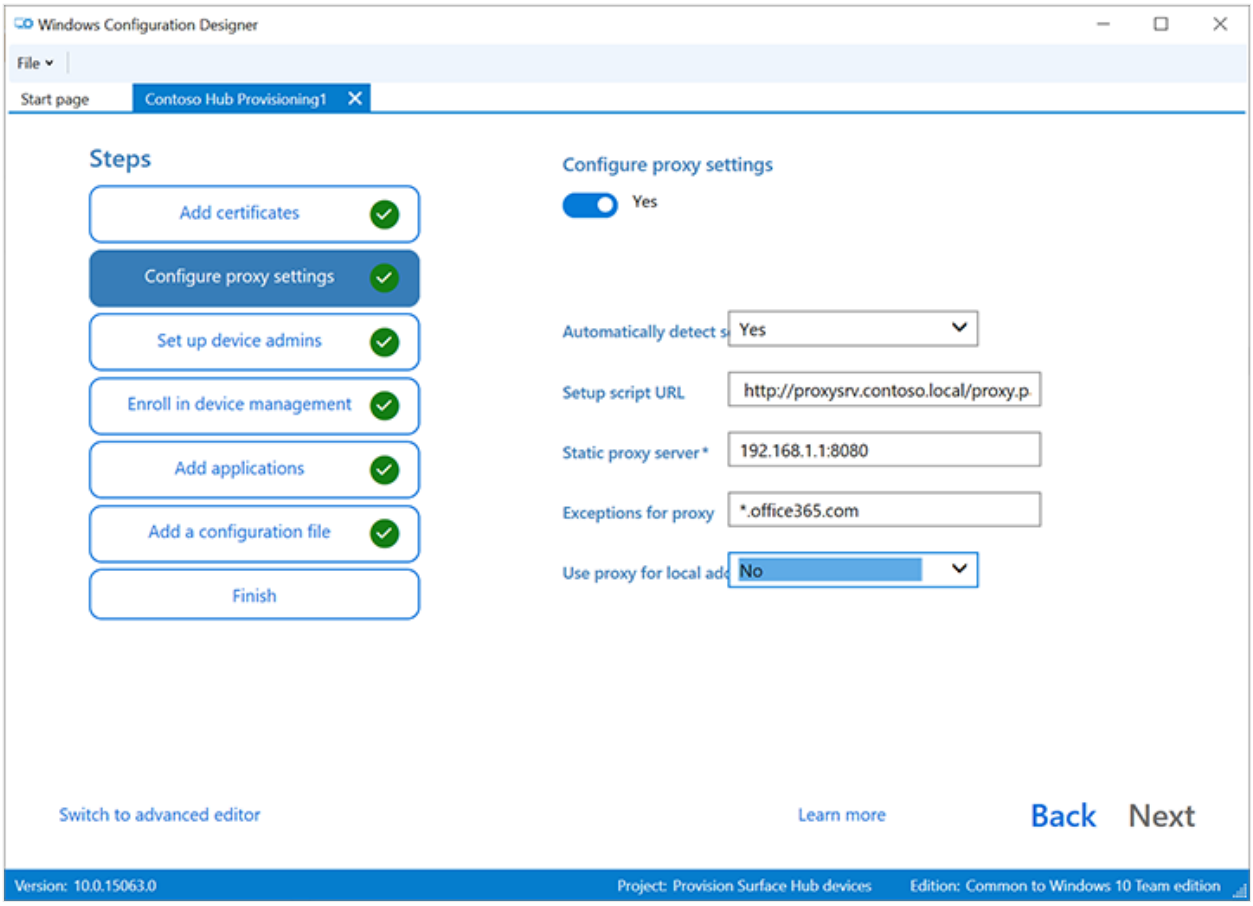
2. Name your project and select **Next**.

Add certificates



To provision the device with a certificate, select **Add a certificate**. Enter a name for the certificate, and then browse to select the certificate to be used. For advanced provisioning options, refer to the section below Add a certificate to your package.

Configure proxy settings



1. Toggle **Yes** or **No** for proxy settings. By default, Surface Hub automatically detects proxy settings. However, if your infrastructure previously required using a proxy server and has changed to not require a proxy server, you can use a provisioning package to revert your Surface Hub devices to the default settings by selecting **Yes** and **Automatically detect settings**.

2. If you toggle **Yes**, you can select to automatically detect proxy settings or manually configure the settings by entering one of the following:

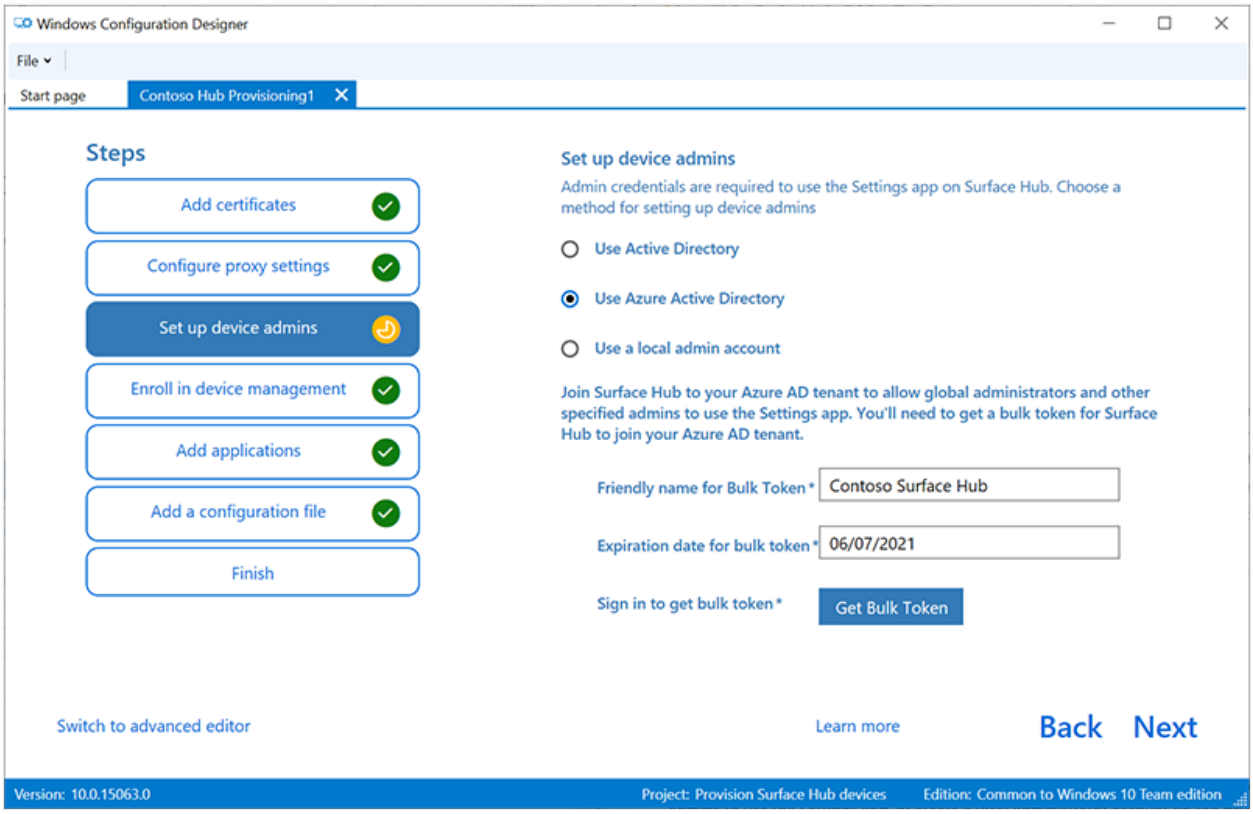
    - A URL to a setup script.
    - A static proxy server address and port information.

3. If you intend to use a setup script or proxy server, turn off **Automatically detect settings**. You can use a setup script *or* a proxy server, not both.

4. Enter exceptions (addresses that Surface Hub should connect to directly without using the proxy server). **Example:** *.office365.com

5. Identify whether to use the proxy server for local addresses.

Set up device admins



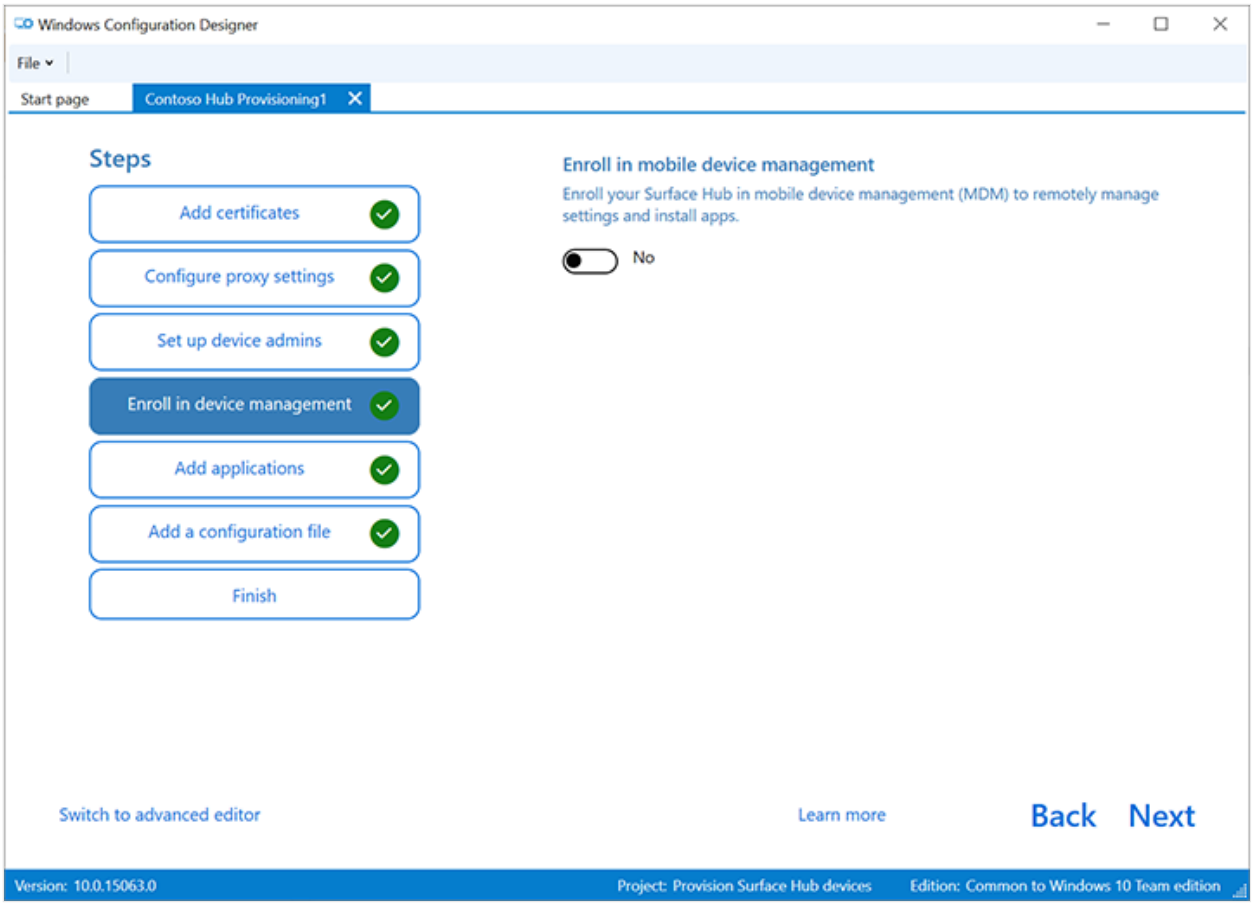
You can enroll the device in Active Directory and specify a security group to use the Settings app, enroll in Azure Active Directory to allow global admins to use the Settings app, or create a local administrator account on the device.

1. To enroll the device in Active Directory, enter the credentials for a least-privileged user account to join the device to the domain, and specify the security group to have admin credentials on Surface Hub. If applying the package to a Surface Hub that was reset, you can use the same domain account as long as it's the same account that set up the Surface Hub initially. Otherwise, a different domain account must be used in the provisioning package.
2. Before you use Windows Configuration Designer to configure bulk Azure AD enrollment, Plan your Azure AD join implementation. The **maximum number of devices per user** setting in your Azure AD tenant determines how many times the bulk token that you get in the wizard can be used.
3. To enroll the device in Azure AD, select that option and enter a friendly name for the bulk token you will obtain using the wizard. Set an expiration date for the token (maximum is 30 days from the date you get the token). Select **Get bulk token**. In the **Let's get you signed in** window, enter an account that has permissions to join a device to Azure AD, and then the password. Select **Accept** to give Windows Configuration Designer the necessary permissions.
4. To create a local administrator account, select that option and enter a user name and password.

> ⓘ **Important**

If you create a local account in the provisioning package, you must change the password using the **Settings** app every 42 days. If the password is not changed during that period, the account might be locked out and unable to sign in.

Enroll in third party MDM provider

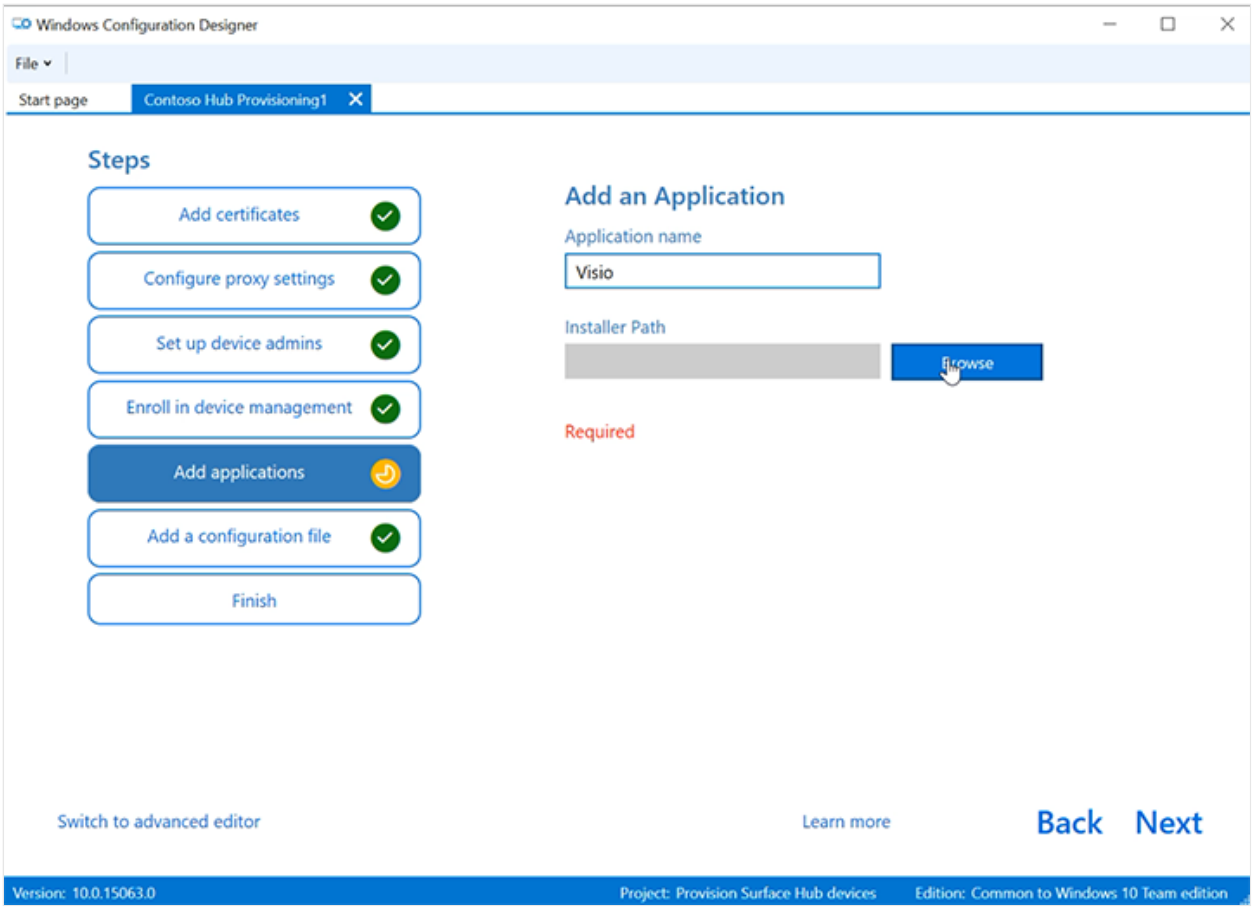


If you use a third party mobile device management (MDM) provider, you can use this section to enroll Surface Hub. To enroll in Intune, first setup Azure AD join, as described in the previous section, and follow the instructions in the following Intune documentation: Quickstart: Set up automatic enrollment for Windows 10/11 devices.

1. Toggle **Yes** or **No** for enrollment in third party MDM.
2. If you toggle **Yes**, provide a service account and password or certificate thumbprint that is authorized to enroll the device and specify the authentication type.
3. If required by your MDM provider, enter the URLs for the discovery service, enrollment service, and policy service.

To learn more, see Manage Surface Hub with an MDM provider.

Add applications



You can install multiple Universal Windows Platform (UWP) apps in a provisioning package. To learn more, see Provision PCs with apps.

> **Note**
>
> Although Windows Configuration Designer lets you add a Classic Win32 app to a provisioning package, Surface Hub only accepts UWP apps. If you include a Classic Win32 app, provisioning will fail.

Password protect provisioning package

If you choose to use a password, you will need to enter it each time you apply the provisioning package to a device.

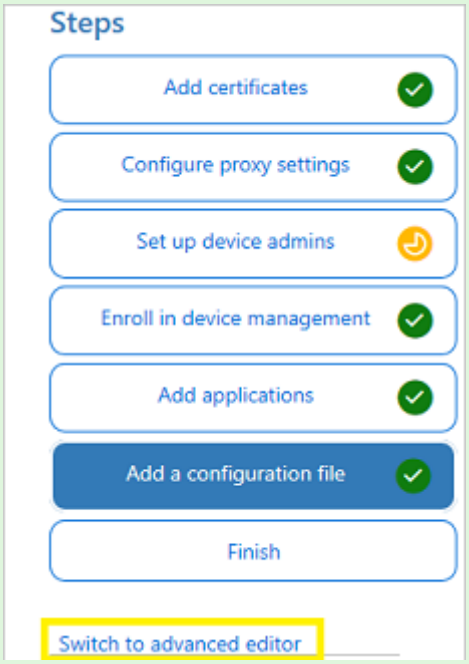
Complete provisioning wizard

If you only need to configure common settings, select **Finish** > **Create** and skip to the section Build your package. Or continue configuring settings by switching to Advanced provisioning.

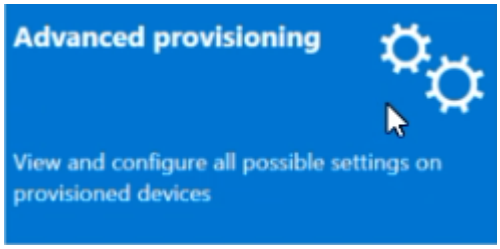
Use Advanced provisioning

Tip

Use the wizard to create a package with the common settings, then switch to the advanced editor to add other settings.

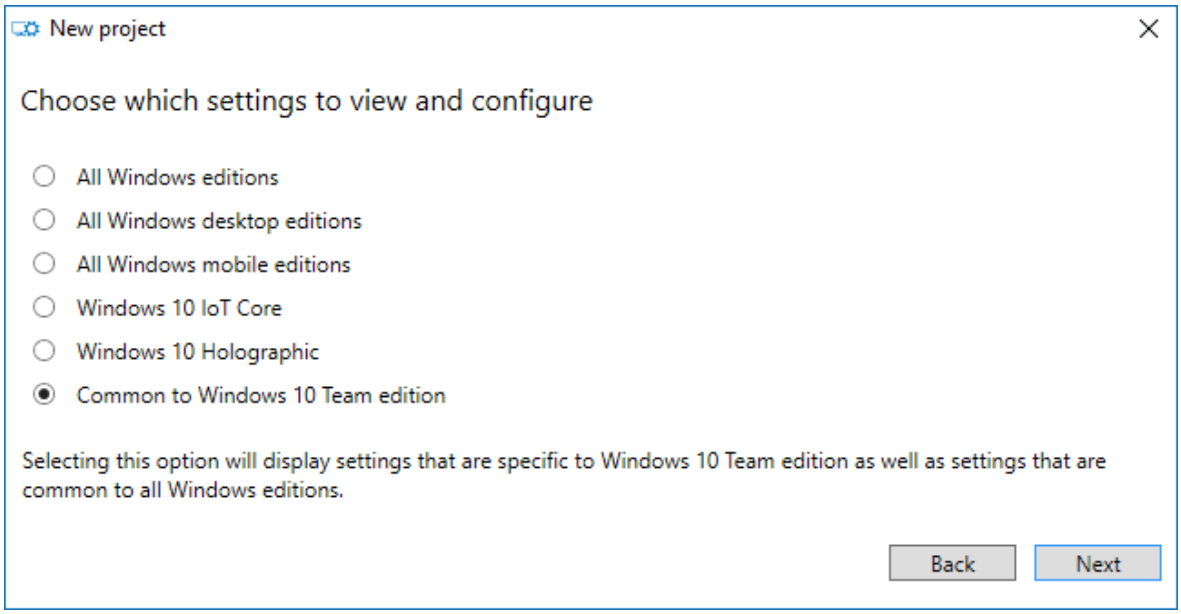


1. If continuing from the previous section, select **Switch to advanced editor** otherwise open **Windows Configuration Designer** and select **Advanced provisioning**.

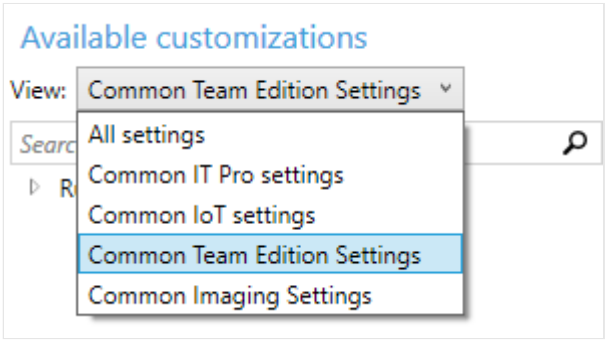


2. Name your project and select **Next**.

3. Select **Common to Windows 10 Team**, select **Next**, and then select **Finish**.



4. In the project, under **Available customizations**, select **Common Team settings**.



Add a certificate to your package

You can use provisioning packages to install certificates that will allow the device to authenticate to Microsoft Exchange.

> **Note**
>
> Provisioning packages can only install certificates to the device (local machine) store, and not to the user store. If your organization requires that certificates be installed to the user store, use the Hub **Settings** app: **Update & Security** > **Certificates** > **Import Certificate**. Alternatively, you can use MDM policies to deploy certificates to either the device store or the user store.

> **Tip**
>
> The **ClientCertificates** section is for .pfx files with a private key; .cer files for root CAs should be placed in the **RootCertificates** section and for Intermediate CAs in the **CACertificates** section.

1. In **Windows Configuration Designer** > **Available customizations** , go to **Runtime settings** > **Certificates** > **ClientCertificates**.
2. Enter a label for **CertificateName** and then select **Add**.
3. Enter the **CertificatePassword**.
4. For **CertificatePath**, browse and select the certificate.
5. Set **ExportCertificate** to **False**.
6. For **KeyLocation**, select **Software only**.

Add a UWP app to your package

To add a UWP app to a provisioning package, you will need the app package (.appx or .appxbundle files) and any dependency files. If you acquired the app from the Microsoft Store for Business, you will also need the *unencoded* app license. See Distribute offline apps to learn how to download these items from the Microsoft Store for Business.

To add a UWP app:

1. In the **Available customizations** pane, go to **Runtime settings** > **UniversalAppInstall** > **DeviceContextApp**.

2. Enter a **PackageFamilyName** for the app and then select **Add**. For consistency, use the app's package family name. If you acquired the app from the Microsoft Store for Business, you can find the package family name in the app license. Open the license file using a text editor, and use the value between the PFM tags.

3. For **ApplicationFile**, select **Browse** to find and select the target app (.appx or .appxbundle).

4. For **DependencyAppxFiles**, select **Browse** to find and add any dependencies for the app. For Surface Hub, you will only need the x64 versions of these dependencies.

If you acquired the app from the Microsoft Store for Business, you will need to add the app license to your provisioning package.

To add app license:

1. Make a copy of the app license, and rename it to use a **.ms-windows-store-license** extension. For example, rename "example.xml" to "example.ms-windows-store-license".

2. In Windows Configuration Designer, go to **Available customizations** > **Runtime settings** > **UniversalAppInstall** > **DeviceContextAppLicense**.

3. Enter a **LicenseProductId** and then select **Add**. For consistency, use the app's license ID from the app license. Open the license file using a text editor. Then, in the **License** tag, use the value in the **LicenseID** attribute.

4. Select the new **LicenseProductId** node. For **LicenseInstall**, select **Browse** to find and select your renamed license file (example.ms-windows-store-license).

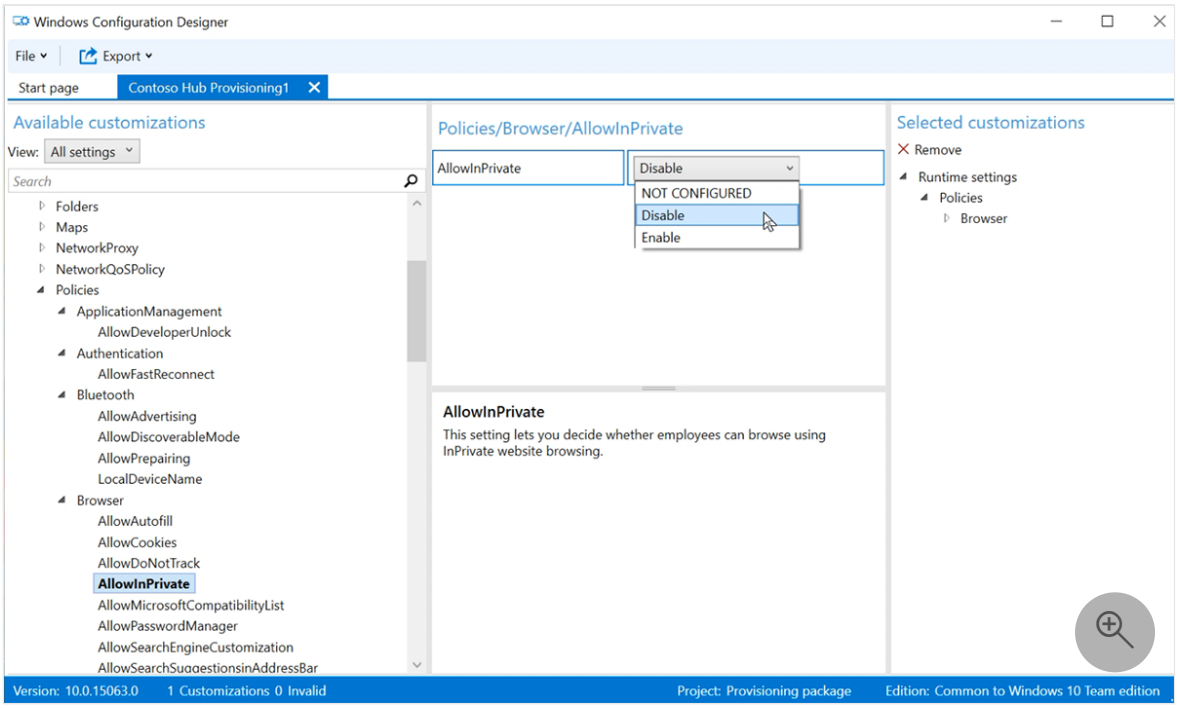
Add a policy to your package

Surface Hub supports a subset of the policies in the Policy configuration service provider. Some of those policies can be configured with Windows Configuration Designer.

To add CSP policies:

1. Go to **Available customizations** > **Runtime settings** > **Policies**.

2. Select the component you want to manage and configure the policy setting as appropriate. For example, to prevent employees from using InPrivate website browsing on Surface Hub, select **AllowInPrivate** and then select **Disable**.



Add Surface Hub settings to your package

You can add settings from the SurfaceHub configuration service provider to your provisioning package.

1. Go to **Available customizations** > **Common Team Edition Settings**.

2. Select the component you want to manage and configure the policy setting as appropriate.
3. When you are done configuring the provisioning package, select **File** > **Save**.
4. Read the warning that project files may contain sensitive information, and select **OK**

Build your package

When you build a provisioning package, you may include sensitive information in the project files and in the provisioning package (.ppkg) file. Although you have the option to encrypt the .ppkg file, project files are not encrypted. Store the project files in a secure location or delete if no longer needed.

1. Open **Windows Configuration Designer** > **Export** > **Provisioning package**.

2. Change **Owner** to **IT Admin**.

3. Set a value for **Package Version**, and then select **Next.**

> **Tip**
>
> Setting the owner to IT Admin ensures that package settings maintain the appropriate "precedence properties" and remain in effect on Surface Hub if other provisioning packages are subsequently applied from other sources.

> **Tip**
>
> You can modify existing packages and change the version number to update previously applied packages.

4. Optional: You can choose to encrypt the package and enable package signing:
   a. Select **Encrypt package** and then enter a password.
   b. Select **Sign package** > **Browse** and choose the certificate as appropriate.

> **Important**
>
> Including a trusted provisioning certificate in your provisioning package is recommended. When the package is applied to a device, the certificate is added to the system store, enabling subsequent packages to be applied silently.

5. Select **Next** to specify the output location. By default, Windows Configuration Designer uses the project folder as the output location. Or select **Browse** to change the default output location. Select **Next**.

6. Select **Build** to start building the package. The project information is displayed in the build page.

7. If your build fails, an error message appears with a link to the project folder. Review the logs to diagnose the error and try building the package again.

8. If your build succeeds, the name of the provisioning package, output directory, and project directory are displayed. Select **Finish** to close the wizard and go back to the Customizations page.

9. Select **output location** to go to the location of the package. Copy the .ppkg to an empty USB flash drive.

Apply a provisioning package to Surface Hub

There are two ways of deploying provisioning packages to a Surface Hub:

- First run setup. You can apply a provisioning package to customize multiple options including Wi-Fi settings, proxy settings, device account details, Azure AD join, and related settings.
- Settings app. After first run setup, you can apply a provisioning package via the Settings app.

Apply a provisioning package during first run

1. When you turn on the Surface Hub for the first time, the first-run program displays the **Hi there page**. Make sure that the settings are properly configured before proceeding.
2. Insert the USB flash drive containing the .ppkg file into the Surface Hub. If the package is in the root directory of the drive, the first-run program will recognize it and ask if you want to set up the device. Select **Set up**.
3. The next screen asks you to select a provisioning source. Select **Removable Media** and tap **Next**.
4. Select the provisioning package (*.ppkg) that you want to apply, and tap **Next**. Note that you can only install one package during first run.
5. The first-run program will show you a summary of the changes that the provisioning package will apply. Select **Yes, add it**.

After the first time the device restarts, remove the USB flash drive. The settings from the provisioning package will be applied to the device and OOBE can be completed.

Apply a provisioning package using Settings app

1. Insert the USB flash drive containing the .ppkg file into the Surface Hub.
2. From Surface Hub, start **Settings** and enter the admin credentials when prompted.
3. Navigate to **Surface Hub** > **Device management**. Under **Provisioning packages**, select **Add or remove a provisioning package** > **Add a package**.
4. Choose your provisioning package and select **Add**. If prompted, enter your admin credentials again.
5. You'll see a summary of the changes to be applied. Select **Yes, add it**.

Learn more

- Download Windows Configuration Designer
- Create a provisioning package
- Manage Surface Hub with an MDM provider

Install apps on Surface Hub

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

You can install additional apps on your Surface Hub to fit your team or organization's needs. There are different methods for installing apps depending on whether you are developing and testing an app, or deploying a released app. This topic describes methods for installing apps for either scenario.

Supported app guidelines

- Surface Hub only runs Universal Windows Platform (UWP) apps. Apps created using the MSIX Packaging Tool will not run on Surface Hub.
- Apps must be targeted for the Universal device family or Windows Team device family.
- Surface Hub only supports offline-licensed apps from Microsoft Store for Business.
- By default, apps must be Store-signed to be installed. During testing and development, you can also choose to run developer-signed UWP apps by placing the device in developer mode.
- When submitting an app to the Microsoft Store, developers need to set Device family availability and Organizational licensing options to make sure an app will be available to run on Surface Hub.
- You need admin credentials to install apps on your Surface Hub. Since the device is designed to be used in communal spaces like meeting rooms, people can't access the Microsoft Store to download and install apps.

Deploy released apps

There are several options for installing apps that have been released to the Microsoft Store, depending on whether you want to evaluate them on a few devices, or deploy them broadly to your organization.

To install released apps:

- Download the app using the Microsoft Store app, or
- Download the app package from the Microsoft Store for Business, and distribute it using a provisioning package or a supported MDM provider.

Microsoft Store app

To evaluate apps released on the Microsoft Store, use the Microsoft Store app on the Surface Hub to browse and download apps.

> **Note**
>
> Using the Microsoft Store app is not the recommended method of deploying apps at scale to your organization:
>
> - To download apps, you must sign in to the Microsoft Store app with a Microsoft account or organizational account. However, you can only connect an account to a maximum of 10 devices at once. If you have more than 10 Surface Hubs, you will need to create multiple accounts or remove devices from your account between app installations.
> - To install apps, you will need to manually sign in to the Microsoft Store app on each Surface Hub you own.

To browse the Microsoft Store on Surface Hub

1. From your Surface Hub, start **Settings**.
2. Type the device admin credentials when prompted.
3. Navigate to **Surface Hub** > **Apps & features**.
4. Select **Open Store** and search for the app you're looking for.

Download app packages from Microsoft Store for Business

To download the app package you need to install apps on your Surface Hub, visit the Microsoft Store for Business. The Store for Business is where you can find, acquire, and manage apps for the Windows 10 devices in your organization, including Surface Hub.

> **Note**
>
> Currently, Surface Hub only supports offline-licensed apps available through the Store for Business. App developers set offline-license availability when they submit apps.

Find and acquire the app you want, then download:

- The offline-licensed app package (either an .appx or an .appxbundle)

- The *unencoded* license file (if you're using provisioning packages to install the app)
- The *encoded* license file (if you're using MDM to distribute the app)
- Any necessary dependency files

For more information, see Download an offline-licensed app.

Install offline-licensed apps via provisioning package

You can manually install the offline-licensed apps that you downloaded from the Store for Business on a few Surface Hubs using provisioning packages. Use Windows Imaging and Configuration Designer (ICD) to create a provisioning package containing the app package and *unencoded* license file that you downloaded from the Store for Business. For more information, see Create provisioning packages for Surface Hub.

Supported MDM provider

To deploy apps to a large number of Surface Hubs in your organization, use a supported MDM provider. The table below shows which MDM providers support deploying offline-licensed app packages.

MDM provider	Supports offline-licensed app packages
On-premises MDM with Configuration Manager (beginning in version 1602)	Yes
Third-party MDM provider	Check to make sure your MDM provider supports deploying offline-licensed app packages.

> **Note**
>
> To deploy offline apps remotely using Microsoft Intune, refer to **Manage VPP apps from Microsoft Store for Business**. Surface Hub app deployment only supports offline apps that are assigned to a Device group and use the Device license type.

Develop and test apps

This section provides information for app developers for testing apps on Surface Hub.

Developer Mode

By default, Surface Hub only runs UWP apps that have been published to and signed by the Microsoft Store. Apps submitted to the Microsoft Store go through security and compliance tests as part of the app certification process, so this helps safeguard your Surface Hub against malicious apps.

By enabling developer mode, you can also install developer-signed UWP apps.

> **Important**
>
> After developer mode has been enabled, you will need to reset the Surface Hub to disable it. Resetting the device removes all local user files and configurations and then reinstalls Windows.

To turn on developer mode

1. From your Surface Hub, start **Settings**.
2. Type the device admin credentials when prompted.
3. Navigate to **Update & security** > **For developers**.
4. Select **Developer mode** and accept the warning prompt.

Visual Studio

During development, the easiest way to test your app on a Surface Hub is using Visual Studio. Visual Studio's remote debugging feature helps you discover issues in your app before deploying it broadly. For more information, see Test Surface Hub apps using Visual Studio.

Create provisioning package

Use Visual Studio to create an app package for your UWP app, signed using a test certificate. Then use Windows Imaging and Configuration Designer (ICD) to create a provisioning package containing the app package. For more information, see Create provisioning packages for Surface Hub.

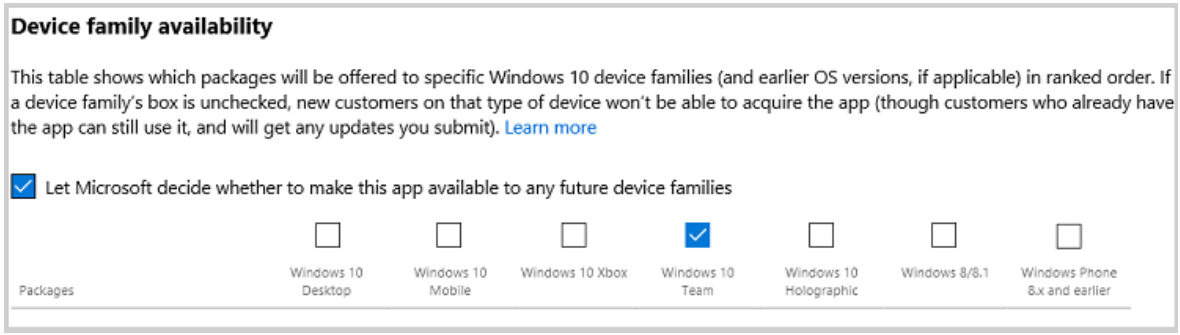
Submit apps to the Microsoft Store

Once an app is ready for release, developers need to submit and publish it to the Microsoft Store. For more information, see Publish Windows apps and games.

During app submission, developers need to set **Device family availability** and **Organizational licensing** options to make sure the app will be available to run on Surface Hub.

To set device family availability

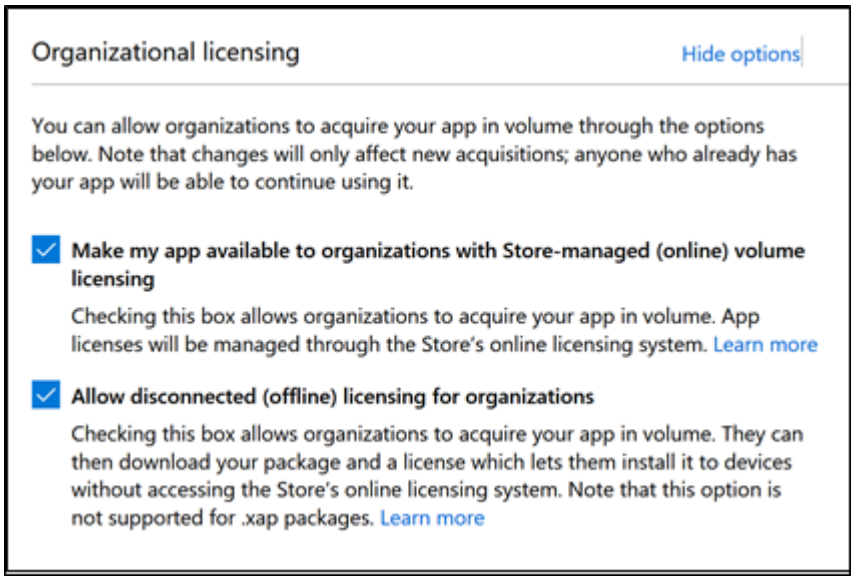
1. On the Windows Dev Center, navigate to your app submission page.
2. Select **Packages**.
3. Under **Device family availability**, select these options:
    - **Windows 10 Team**
    - **Let Microsoft decide whether to make the app available to any future device families**



For more information, see Device family availability.

To set organizational licensing

1. On the Windows Dev Center, navigate to your app submission page.
2. Select **Pricing and availability**.
3. Under Organizational licensing, select **Allow disconnected (offline) licensing for organizations**.



> **Note**
>
> **Make my app available to organizations with Store-managed (online) licensing and distribution** is selected by default.

> **Note**
>
> Developers can also publish line-of-business apps directly to enterprises without making them broadly available in the Store. For more information, see **Distribute LOB apps to enterprises**.

For more information, see Organizational licensing options.

Summary

There are a few different ways to install apps on your Surface Hub depending on whether you are developing apps, evaluating apps on a small number of devices, or deploying apps broadly to your organization. This table summarizes the supported methods:

Install method	Developing apps	Evaluating apps on a few devices	Deploying apps broadly to your organization
Visual Studio	X		
Provisioning package	X	X	
Microsoft Store app		X	

Install method	Developing apps	Evaluating apps on a few devices	Deploying apps broadly to your organization
Supported MDM provider			X

Install Progressive Web Apps on Surface Hub

Article • 03/21/2023

Progressive Web App (PWA) support opens up a rich new source of apps that significantly extends the library of available apps that can run on Surface Hub. Users can access a wealth of applications outside of the Microsoft Store and run them directly from the App menu. Compared to web pages, PWAs behave more like native apps with offline functionality, the ability to update in the background, and other unique features. Most websites can be installed as PWAs and take advantage of any additional functionality enabled by web developers.

Admins can remotely install PWAs on Surface Hubs via mobile device management (MDM) providers like Microsoft Intune. Or you can use a provisioning pack. This article describes both methods with sample code for installing YouTube, WebEx, Zoom, and Uber and instructions for installing your own PWAs. To learn more, see Overview of Progressive Web Apps.

> **Note**
>
> Before you install PWAs, ensure that your Surface Hub has **KB5011543** (or a subsequent Windows update) installed. To learn more about the latest Windows 10 Team updates, refer to **Surface Hub update history**.

- Install PWAs on Surface Hub via Intune
- Install PWAs on Surface Hub via provisioning package

Users can also install PWAs for use during their Hub session. When the session ends, PWAs are removed. To learn more, see Install, manage, or uninstall apps in Microsoft Edge

Install PWAs via Intune

Use Intune or another MDM provider to install PWAs on Surface Hubs. To learn more, refer to Manage Surface Hub with an MDM provider.

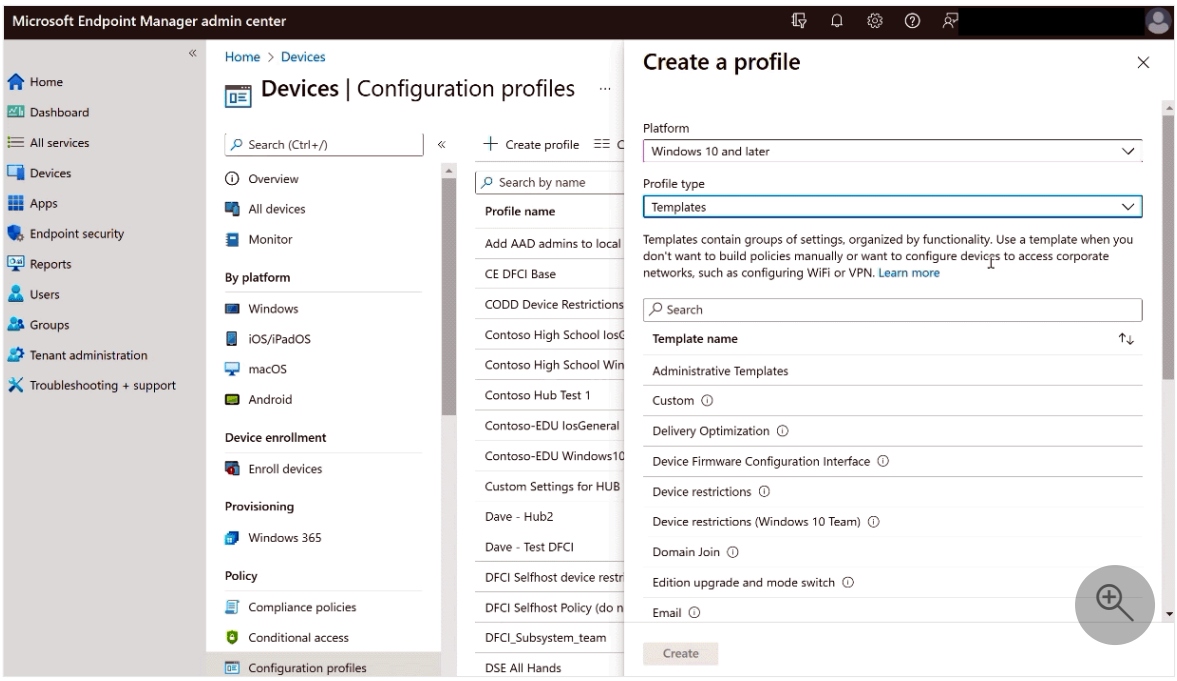
Get started

1. Sign in to the Intune portal at **Microsoft Intune admin center**.

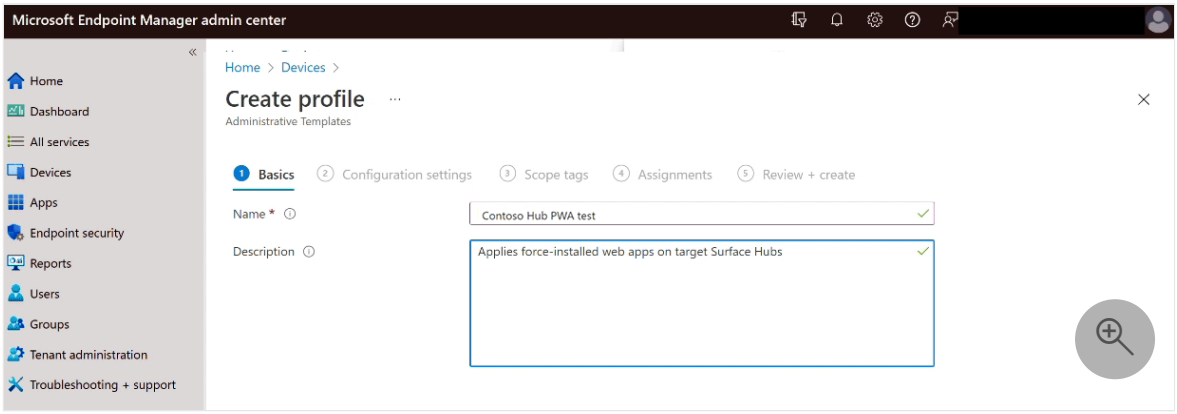
2. Go to **Devices** > **Configuration Policies** > **Create profile**.

3. Under Platform, select **Windows 10 and later**. Under Profile type, select **Templates**. Under Template name, select **Administrative Templates.**

4. Select **Create.**

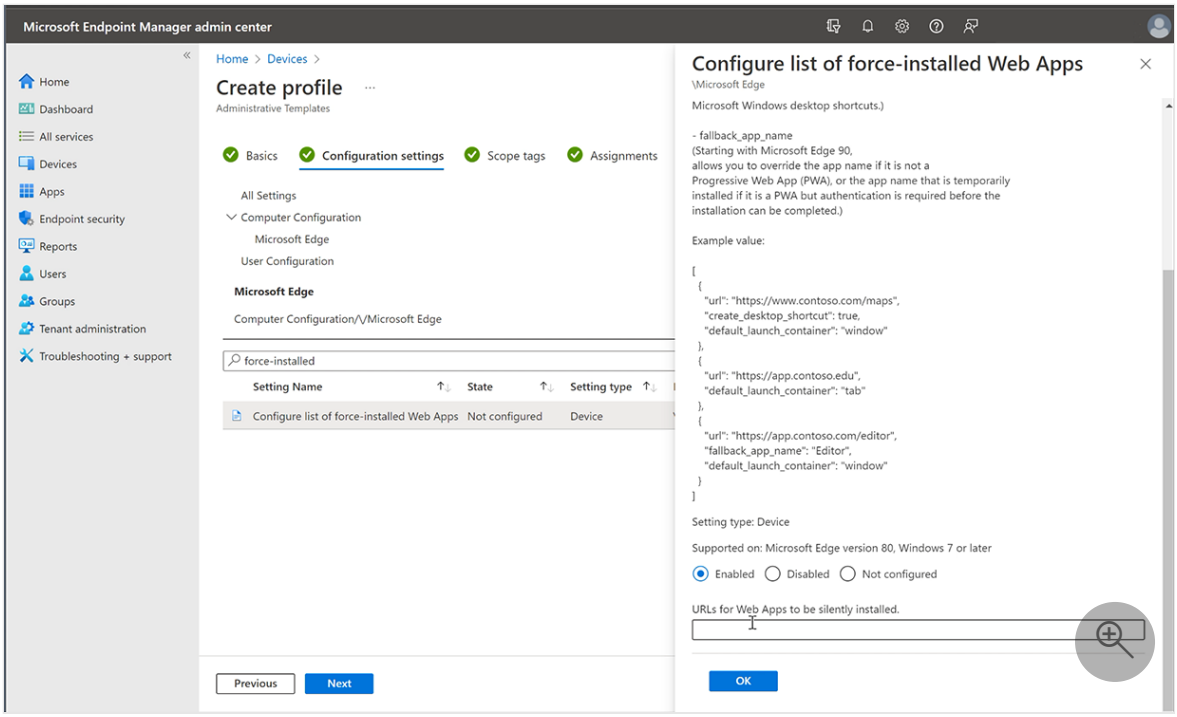


5. Name the profile, enter an optional description, and select **Next**.

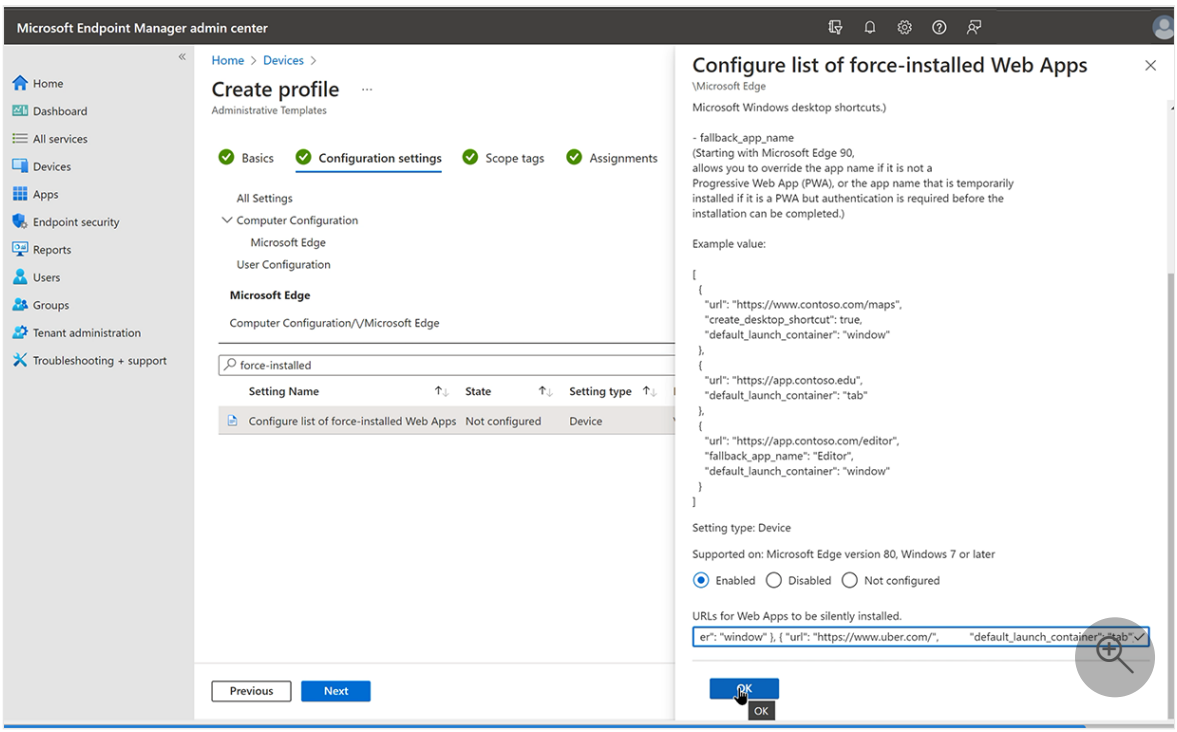


Configure force-installed Web Apps policy (Intune)

1. Under **All Settings** > **Computer Configuration**, select **Microsoft Edge** and in the Search box, enter **force-installed**, select **force-installed Web Apps**, and then select **Enabled**.



2. Under **URLs for Web Apps to be silently installed**, copy and enter the following code snippet to install PWAs for YouTube, Webex, Zoom, and Uber. Or skip to the next step to install other PWAs.



JSON

```
[
{ "url": "https://www.youtube.com/",       "default_launch_container":
"window" },
{ "url": "https://signin.webex.com/join",  "default_launch_container":
"window" },
{ "url": "https://zoom.us/join",           "default_launch_container":
"window" },
```

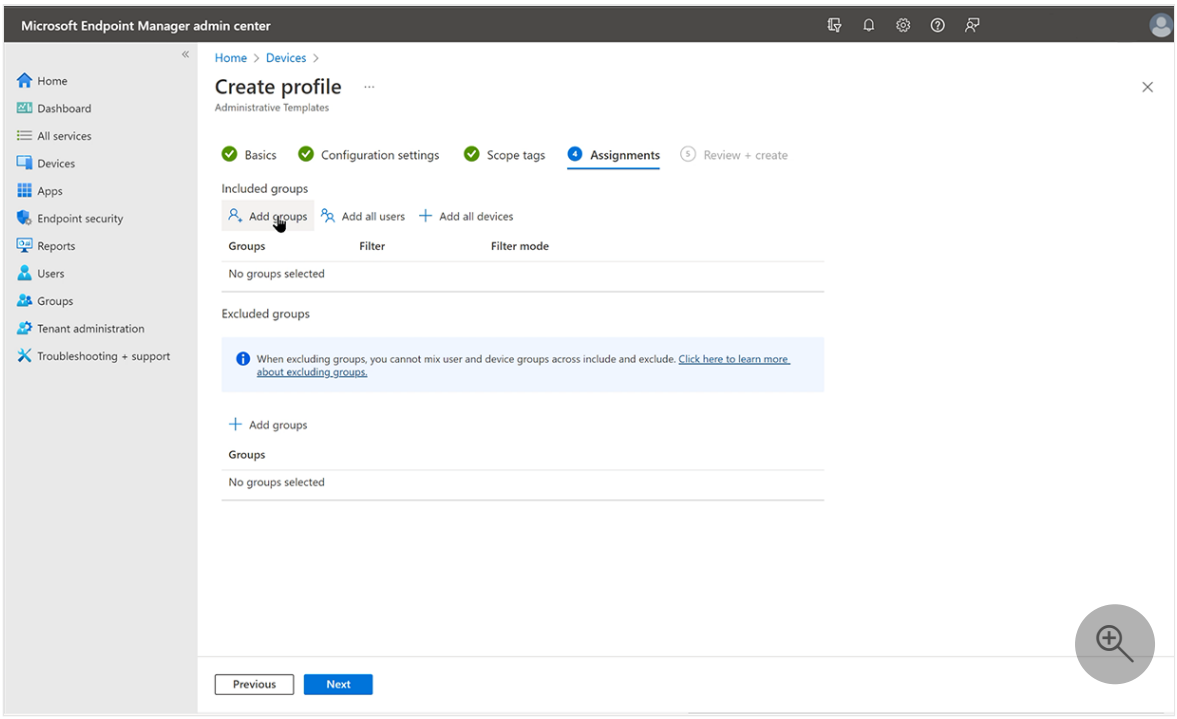
```
{ "url": "https://www.uber.com/",          "default_launch_container":
"tab"}
]
```

3. Alternatively, you can create a JSON snippet from the following syntax to install other PWAs.

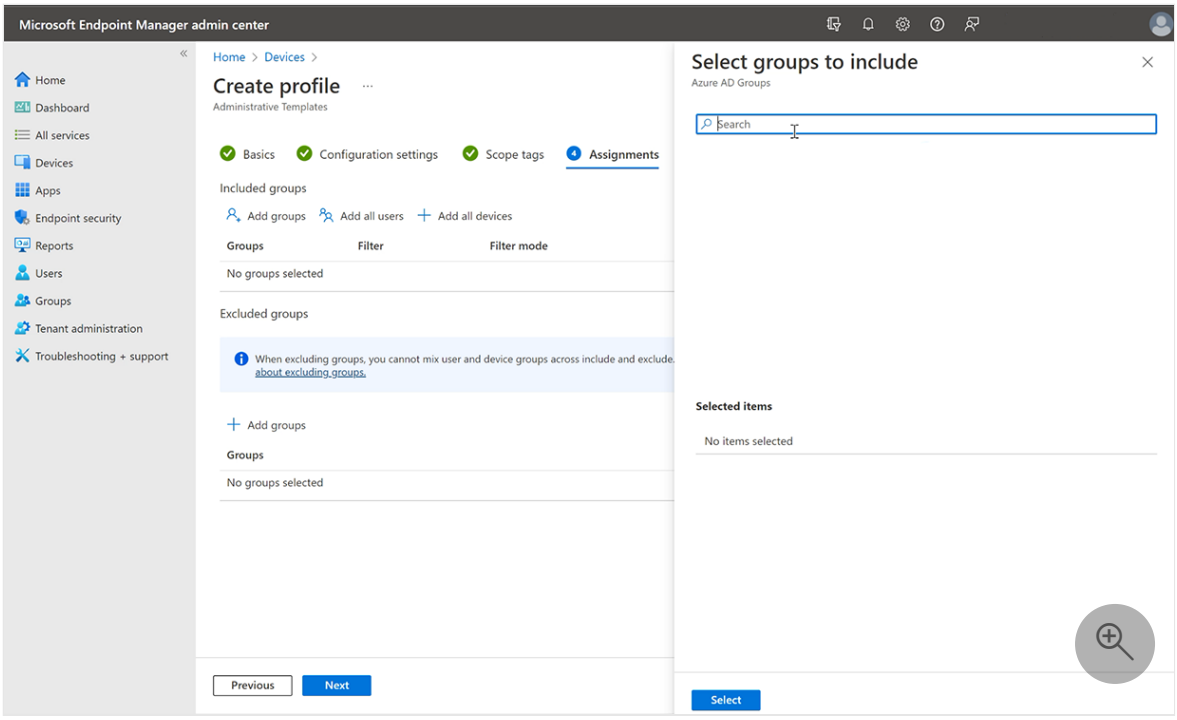
```
JSON

[ { "url": "https://www.contoso.com ",    "default_launch_container":
"window" },

{ "url": "https://www.fabrikam.com/",    "default_launch_container":
"tab"   } ]
```

4. On the Scope tags page, select **Next** to skip.

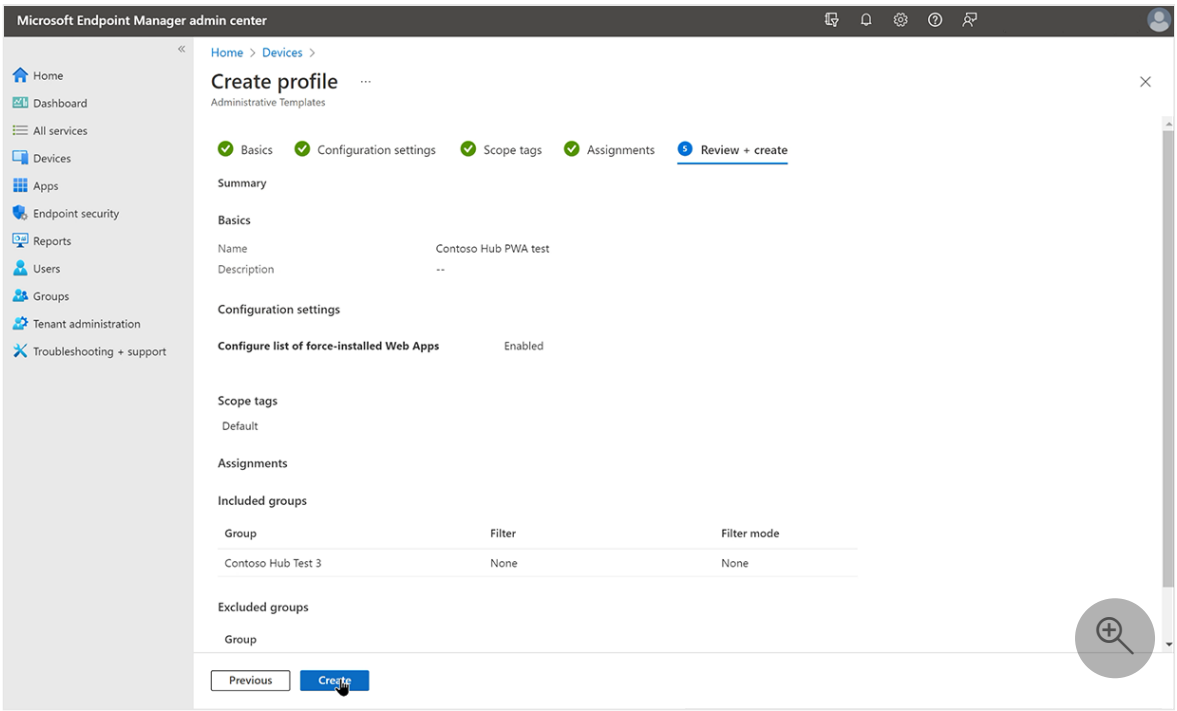
5. On the Assignments page, under **Included groups**, select **Add groups**.



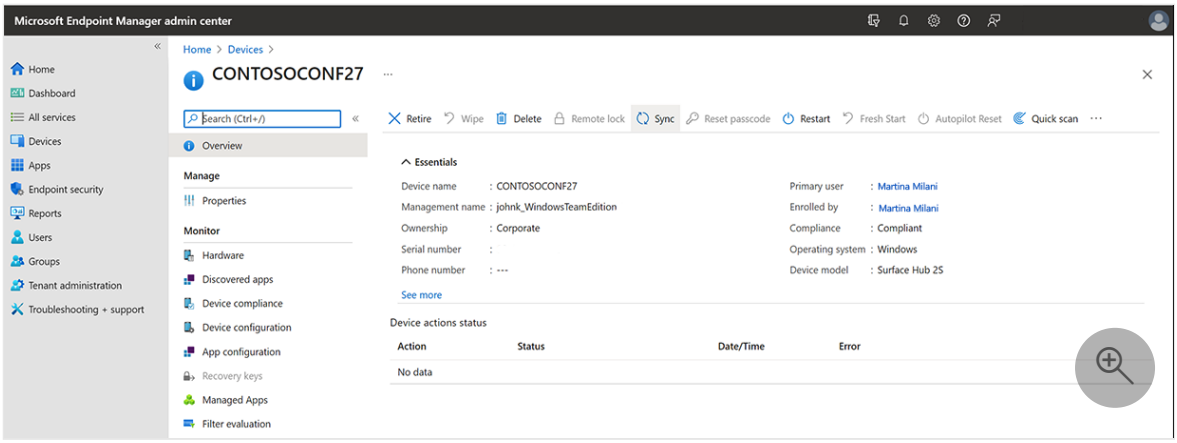
6. Under **Select groups to include**, enter the name of a group containing the Surface Hubs you wish to target, choose **Select**, and then click **Next**. To learn more about assigning a Configuration profile to a group, see Add groups to organize users and devices.



7. Review and then select **Create**.



8. To apply the Configuration profile immediately, select **Devices** > **All devices** and find the device you targeted. Open its Overview pane, and select **Sync**.



> **Important**
>
> To complete installation of PWAs, go to your Surface Hub and launch Edge. PWAs are installed and appear in the Start menu All apps list.

Add PWAs to Start menu

You can modify the default Start menu so users have quick access to PWAs at the start of each Surface Hub session. To learn more, see Configure Surface Hub Start menu

Troubleshooting Intune-managed PWAs

If you don't see PWAs listed under **All apps:**

- Make sure your Surface Hub has the latest updates, specifically KB5011543 (or a subsequent Windows update). To learn more about the latest Windows 10 Team updates, refer to Surface Hub update history.
- Check to ensure the Configuration profile has successfully applied and has no conflicts with other settings.
- Check to ensure the Configuration profile is targeted to a security group that contains your Surface Hub.
- Remember to launch Edge a single time on your Surface Hub, which is required for Intune-managed PWAs to successfully install.

Install PWAs via provisioning package

You can install PWAs by applying a provisioning package to Surface Hubs using a USB drive. To learn more refer to Create provisioning packages.

Get started with provisioning

1. On a separate PC running Windows 10 or Windows 11, install Windows Configuration Designer (WCD) from the Microsoft Store.

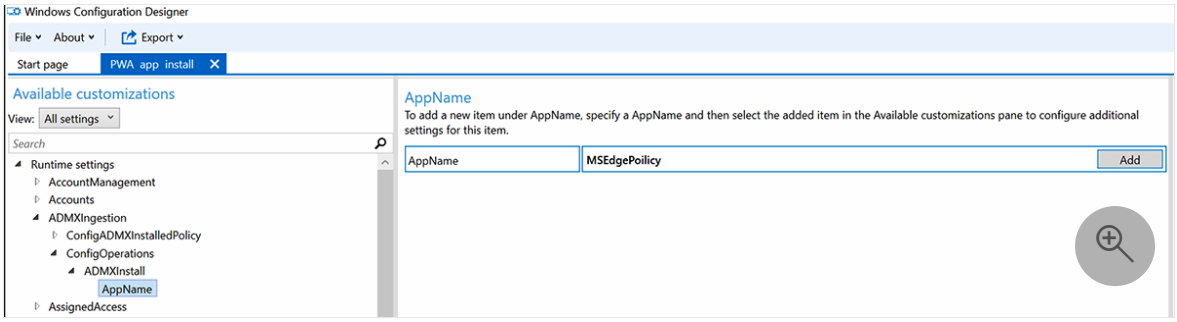
2. In WCD, create a new Project. Select **Provision Desktop Devices,** provide a name for the project and choose **Finish.**

3. Select **Switch to advanced editor** and select **Yes** to confirm.

Configure MSEdgePolicy

1. In the Available customizations pane in WCD, go to **\Runtime Settings\ADMXIngestion\ConfigOperations\ADMXInstall\AppName**

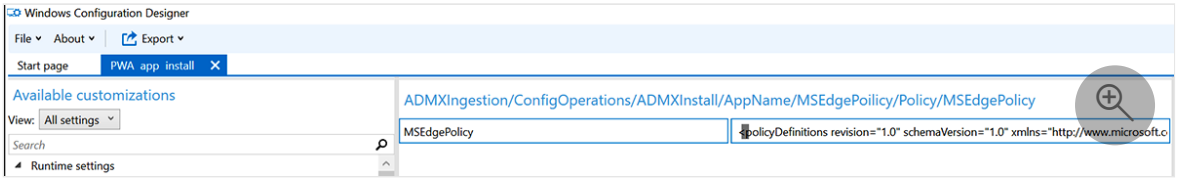
2. In the customizations edit pane, enter the app name as **MSEdgePolicy** and select **Add**.



3. In the Available customizations pane, select **AppName: MSEdgePolicy** and in the edit pane, change **SettingType** to **Policy** and choose **Add**.

4. In the Available customizations pane, select **SettingType: Policy** and in the edit pane, set **AdmxFileUid** to **MSEdgePolicy,** and choose **Add**.

5. In the Available customizations pane, select **AdmxFileUid: MSEdgePolicy** and in the edit pane, set **MSEdgePolicy** by entering the following code as a single line of text:



XML

```
<policyDefinitions revision="1.0" schemaVersion="1.0"
xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">  <!--
microsoft_edge version: 96.0.1054.53-->  <policyNamespaces>    <target
namespace="Microsoft.Policies.Edge" prefix="microsoft_edge"/>    <using
namespace="Microsoft.Policies.Windows" prefix="windows"/>
```

```
</policyNamespaces>  <resources minRequiredRevision="1.0"/>
<supportedOn>    <definitions>      <definition
displayName="$(string.SUPPORTED_WIN7_V80)" name="SUPPORTED_WIN7_V80"/>
</definitions>  </supportedOn>  <categories>    <category
displayName="$(string.microsoft_edge)" name="microsoft_edge"/>
<category displayName="$(string.microsoft_edge_recommended)"
name="microsoft_edge_recommended"/>  </categories>  <policies>
<policy class="Both" displayName="$(string.WebAppInstallForceList)"
explainText="$(string.WebAppInstallForceList_Explain)"
key="Software\Policies\Microsoft\Edge" name="WebAppInstallForceList"
presentation="$(presentation.WebAppInstallForceList)">
<parentCategory ref="microsoft_edge"/>      <supportedOn
ref="SUPPORTED_WIN7_V80"/>      <elements>        <text
id="WebAppInstallForceList" maxLength="1000000"
valueName="WebAppInstallForceList"/>      </elements>    </policy>
</policies></policyDefinitions>
```

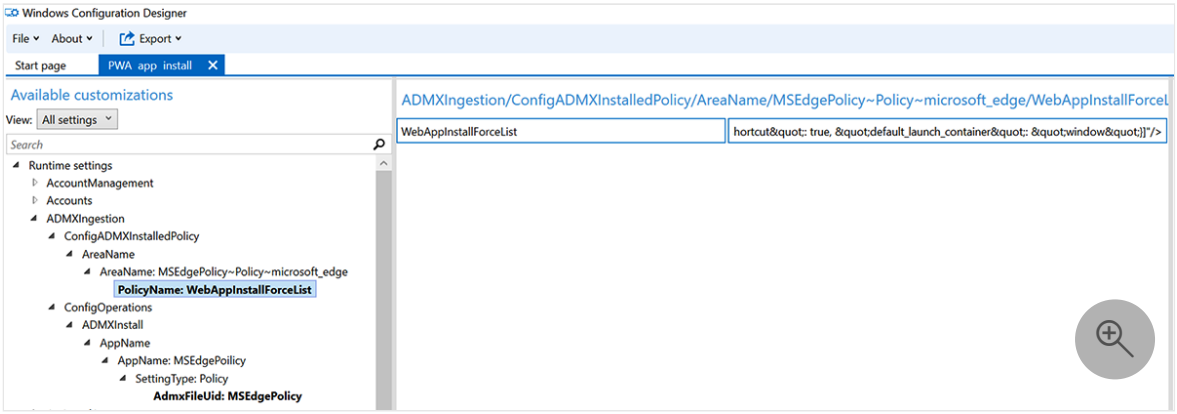
Configure force-installed Web Apps policy (provisioning package)

1. In the Available customizations pane in WCD, go to: **\Runtime Settings\ADMXIngestion\ConfigADMXInstalledPolicy\AreaName**

2. In the customizations edit pane, enter the Areaname as **MSEdgePolicy~Policy~microsoft_edge,** select **Add**.

3. In the Available customizations pane, select **AreaName: MSEdgePolicy~Policy~microsoft_edge** and in the edit pane, set **Policy Name** to **WebAppInstallForceList** and select **Add**.

4. In the Available customizations pane, select **PolicyName: WebAppInstallForceList** and in the edit pane for **WebAppInstallForceList** enter PWA code as a single line of text.



PPKG code samples

- YouTube PWA:

```
XML

<enabled/><data id="WebAppInstallForceList" value="[{&amp;quot;url&amp;quot;:
&amp;quot;https://www.youtube.com&amp;quot;,
&amp;quot;create_desktop_shortcut&amp;quot;: true,
&amp;quot;default_launch_container&amp;quot;: &amp;quot;window&amp;quot;}]"/>
```

- Multiple PWAs including YouTube, Webex, Zoom, and Uber:

```
XML

 <enabled/><data id="WebAppInstallForceList" value="[{&amp;quot;url&amp;quot;:
&amp;quot;https://www.youtube.com&amp;quot;,
&amp;quot;create_desktop_shortcut&amp;quot;: true,
&amp;quot;default_launch_container&amp;quot;: &amp;quot;window&amp;quot;},
{&amp;quot;url&amp;quot;: &amp;quot;https://signin.webex.com/join&amp;quot;,
&amp;quot;create_desktop_shortcut&amp;quot;: true,
&amp;quot;default_launch_container&amp;quot;: &amp;quot;window&amp;quot;},
{&amp;quot;url&amp;quot;: &amp;quot;https://zoom.us/join&amp;quot;,
&amp;quot;create_desktop_shortcut&amp;quot;: true,
&amp;quot;default_launch_container&amp;quot;: &amp;quot;window&amp;quot;},
{&amp;quot;url&amp;quot;: &amp;quot;https://www.uber.com&amp;quot;,
&amp;quot;create_desktop_shortcut&amp;quot;: true,
&amp;quot;default_launch_container&amp;quot;: &amp;quot;window&amp;quot;}]"/>
```

- Alternatively, you can create a JSON snippet from the following syntax to install other PWAs:

```
XML

<enabled/><data id="WebAppInstallForceList" value="[{&amp;quot;url&amp;quot;:
&amp;quot;https://www.contoso.com&amp;quot;,
&amp;quot;create_desktop_shortcut&amp;quot;: true,
&amp;quot;default_launch_container&amp;quot;: &amp;quot;window&amp;quot;}]"/>
```

Export provisioning package and apply to Surface Hubs

1. In the menu bar, select **Export**, select **Provisioning Package** and follow the prompts to generate the .ppkg file.
2. Insert an empty USB flash drive. Select output location to go to the location of the package. Copy the .ppkg file to the USB drive.
3. Apply the provisioning package via the Settings app or during first-run setup. To learn more, see Create provisioning packages

Troubleshooting provisioning package PWAs

If you don't see PWAs listed under **All apps**:

- Make sure your Surface Hub has the latest updates, specifically KB5011543 (or a subsequent Windows update). To learn more about the latest Windows 10 Team updates, refer to Surface Hub update history.

Related links

- Configure Surface Hub Start menu
- WCD reference: ADMXIngestion
- Overview of Progressive Web Apps (PWAs)

Connect devices to Surface Hub 2S

Article • 05/11/2023

Surface Hub 2S enables you to connect external devices, mirror the display on Surface Hub 2S to another device, and connect multiple third-party peripherals including video conference cameras, conference phones, and room system devices.

You can display content from your devices to Surface Hub 2S. If the source device is Windows-based, that device can also provide TouchBack and InkBack, which takes video and audio from the connected device and presents them on Surface Hub 2S. If Surface Hub 2S encounters a High-Bandwidth Digital Content Protection (HDCP) signal, such as a Blu-ray DVD player, the source is displayed as a black image.

> **Note**
>
> Surface Hub 2S uses the video input selected until a new connection is made, the existing connection is disrupted, or the Connect app is closed.

Project using cables to Surface Hub 2S

To project your screen with cables, connect using the ports along the bottom edge of the compute cartridge. The compute cartridge has an HDMI port, a USB-C port, USB-A, as well as the Ethernet port and DisplayPort.

You can project in with USB-C or HDMI—the DisplayPort is only for mirroring your Surface Hub's screen on another screen.

Recommended wired configurations

In general, it's recommended to use native cable connections whenever possible such as USB-C to USB-C or HDMI to HDMI. Other combinations such as MiniDP to HDMI or MiniDP to USB-C will also work. Some additional configuration may be required to optimize the video-out experience, as described on this page.

Connection	Functionality	Description
HDMI + USB-C	HDMI-in for audio and video USB-C for TouchBack and InkBack	USB-C supports TouchBack and InkBack with the HDMI A/V connection. Use USB-C to USB-A to connect to legacy computers. **NOTE:** For best results, connect HDMI before connecting a USB-C cable. If the computer you're using for HDMI is not compatible with TouchBack and InkBack, you won't need a USB-C cable.
USB-C (via compute module)	Video-in Audio-in	Single cable needed for A/V TouchBack and InkBack is supported HDCP enabled
HDMI (in port)	Video, Audio into Surface Hub 2S	Single cable needed for A/V TouchBack and InkBack not supported HDCP enabled
MiniDP 1.2 output	Video-out such as mirroring to a larger projector.	Single cable needed for A/V

When you connect a guest computer to Surface Hub 2S via the USB-C port, several USB devices are discovered and configured. These peripheral devices are created for TouchBack and InkBack. As shown in the following table, the peripheral devices can be viewed in Device Manager, which will show duplicate names for some devices, as shown in the following table.

Peripheral	Listing in Device Manager

Peripheral	Listing in Device Manager
Human interface devices	HID-compliant consumer control device HID-compliant pen HID-compliant pen (duplicate item) HID-compliant pen (duplicate item) HID-compliant touch screen USB Input Device USB Input Device (duplicate item)
Keyboards	Standard PS/2 keyboard
Mice and other pointing devices	HID-compliant mouse
USB controllers	Generic USB hub USB composite device

Connect video-in to Surface Hub 2S

You can input video to Surface Hub 2S using USB-C or HDMI, as indicated in the following table.

Surface Hub 2S video-in settings

Signal Type	Resolution	Frame rate	HDMI	USB-C
PC	640 x 480	60	X	X
PC	720 x 480	60	X	X
PC	1024 x 768	60	X	X
PC	1920 x 1080	60	X	X
PC	3840x2560	30	X	X
HDTV	720p	60	X	X
HDTV	1080p	60	X	X
4K UHD	3840x2560	30	X	X

> ⓘ **Note**
>
> The 4K UHD resolution (3840×2560) is only supported when connecting to ports on the compute module. It is not supported on the “guest” USB ports located on the left, top, and right sides of the device.

> **Note**
>
> Video from a connected external PC may appear smaller when displayed on Surface Hub 2S.

Mirror Surface Hub 2S display on another device

You can output video to another display using MiniDP, as indicated in the following table.

Surface Hub 2S video-out settings

Signal Type	Resolution	Frame rate	MiniDP
PC	640 x 480	60	X
PC	720 x 480	60	X
PC	1024 x 768	60	X
PC	1920 x 1080	60	X
PC	3840 x 2560	60	X
HDTV	720p	60	X
HDTV	1080p	60	X
4K UHD	3840 x 2560	60	X

Surface Hub 2S includes a MiniDP video-out port for projecting visual content from Surface Hub 2S to another display. If you plan to use Surface Hub 2S to project to another display, note the following recommendations:

- **Keyboard required.** Before you begin, you'll need to connect either a wired or Bluetooth-enabled external keyboard to Surface Hub 2S. Note that unlike the original Surface Hub, a keyboard for Surface Hub 2S is sold separately and is not included in the shipping package.

- **Set duplicate mode.** Surface Hub 2S supports video-out in duplicate mode only. However, you will still need to manually configure the display mode when you

connect for the first time:

1. Enter the **Windows logo key** + **P**, which opens the Project pane on the right side of Surface Hub 2S, and then select **Duplicate** mode.
2. When you're finished with your Surface Hub 2S session, select **End Session**. This ensures that the duplicate setting is saved for the next session.

- **Plan for different aspect ratios.** Like other Surface devices, Surface Hub 2S uses a 3:2 display aspect ratio (the relationship between the width and the height of the display). Projecting Surface Hub 2S onto displays with different aspect ratios is supported. Note however that because Surface Hub 2S duplicates the display, the MiniDP output will also only display in a 3:2 aspect ratio, which may result in letterboxing or curtaining depending on the aspect ratio of the receiving display.

> ⓘ **Note**
>
> if your second monitor uses a 16:9 aspect ratio (the predominant ratio for most TV monitors), black bars may appear on the left and right sides of the mirrored display. If this occurs, you may wish to inform your users that there is no need to adjust the second display.

Select cables

Note the following recommendations:

- **USB.** USB 3.1 Gen 2 cables.
- **MiniDP.** DisplayPort cables certified for up to 3 meters in length.
- **HDMI.** If a long cable is necessary, HDMI is recommended due to the wide availability of cost-effective, long-haul cables with the ability to install repeaters if needed.

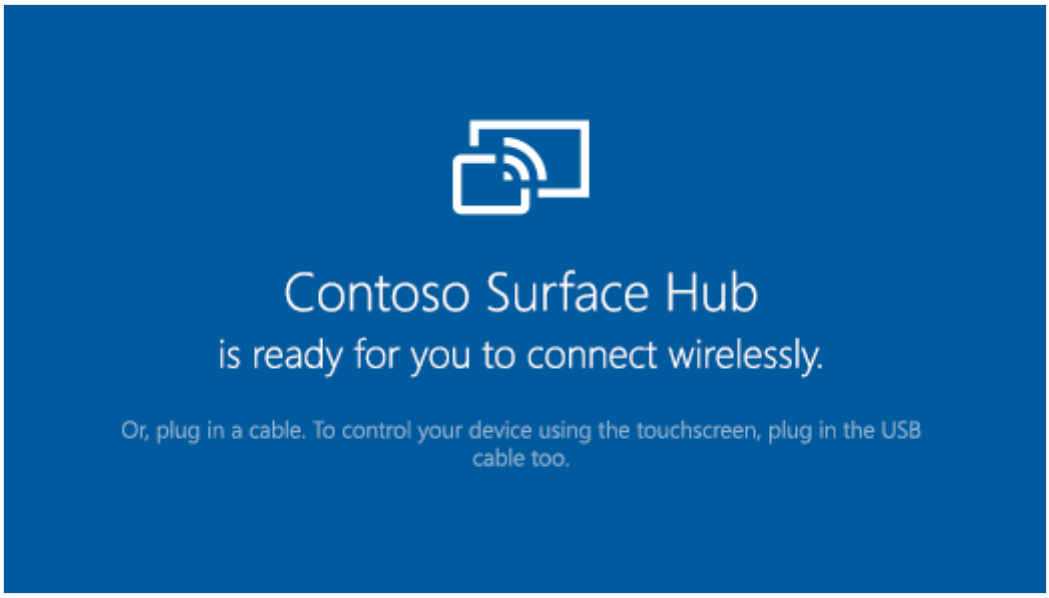
> 💡 **Tip**
>
> Most DisplayPort sources will automatically switch to HDMI signaling if HDMI is detected.

Wirelessly connect to Surface Hub 2S

Windows 10/11 natively supports Miracast, which lets you wireless connect to Surface Hub 2S.

To connect using Miracast:

1. On your Windows 10/11 device, enter **Windows logo key** + **K**.
2. In the Connect window, look for the name of your Surface Hub 2S in the list of nearby devices. You can find the name of your Surface Hub 2S in the bottom left corner of the display or when you press **Connect** on the welcome screen.



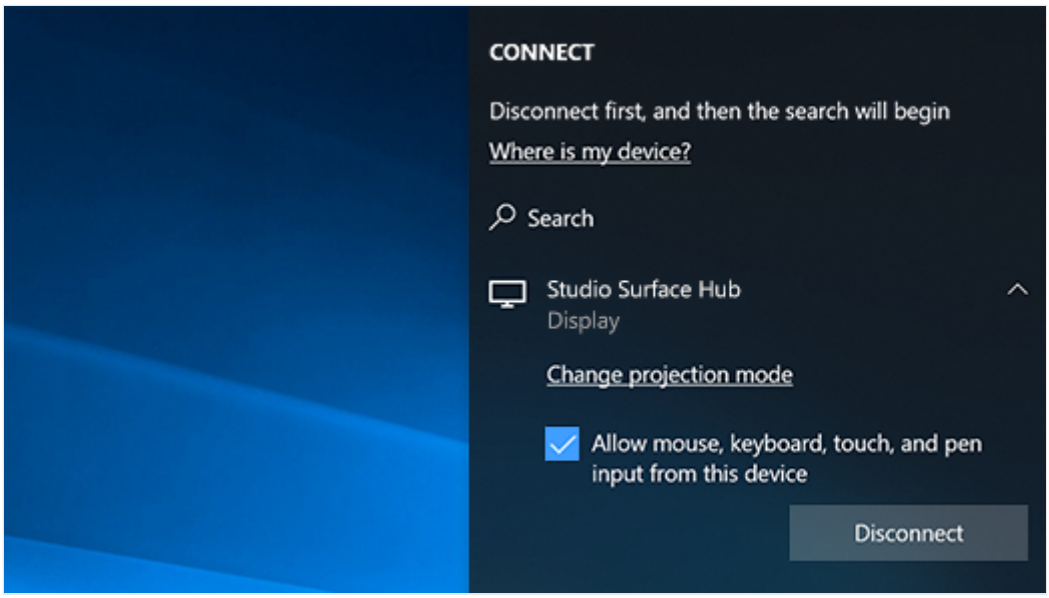
3. Enter a PIN if your system administrator has enabled the PIN setting for Miracast connections. This requires you to enter a PIN number when you connect to Surface Hub 2S for the first time.

> ⓘ **Note**
>
> If you do not see the name of the Surface Hub 2S device as expected, it's possible the previous session was prematurely closed. If so, sign into Surface Hub 2S directly to end the previous session and then connect from your external device.

Control your laptop from the Surface Hub

Sometimes when you're presenting or collaborating on Surface Hub, you'll want to be able to leave your laptop at your seat and be able to fully pay attention to what's on the big screen.

When you've connected a device that has Windows 8 or later to Surface Hub, on that device, you'll see a checkbox to **Allow mouse, keyboard, touch, and pen input**.



When this is checked, you'll be able to use touch and inking on the Surface Hub to control and make changes on your own connected device. If you're connecting via USB-C, you'll be able to use the touch and inking to make changes on your device automatically. However, if you're connecting with HDMI, you'll need to connect a USB cable as well to use touch and pen input on your device.

Connect peripherals to Surface Hub 2S

Bluetooth accessories

You can connect the following accessories to Surface Hub-2S using Bluetooth:

- Mice
- Keyboards
- Headsets
- Speakers
- Surface Hub 2 pens

> **Tip**
>
> After you connect a Bluetooth headset or speaker, you might need to change the default microphone and speaker settings. For more information, see **Local management for Surface Hub settings**.

Connect other devices and display with Surface Hub

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

You can connect other devices to your Microsoft Surface Hub to display content. This article describes the Guest Mode, Replacement PC Mode, and Video Out functionality available through wired connections, and also lists accessories that you can connect to Surface Hub using Bluetooth.

> **Tip**
>
> Surface Hub will use the video input that you select until a new connection is made, the existing connection is disrupted, or the Connect App is closed.

Which method should I choose?

When connecting external devices and displays to a Surface Hub, there are several available options. The method you use depends on your scenario and needs.

When you want to:	Use this method:
Mirror the Surface Hub's display on another device.	Video Out
Present another device's display on the Surface Hub screen and interact with both the device's content and the built-in Surface Hub experience.	Guest Mode
Power the Surface Hub from an external Windows 10 or Windows 11 PC, turning off the embedded computer of the Surface Hub. Cameras, microphones, speakers, and other peripherals, are sent to the external PC, in addition to pen and touch.	Replacement PC Mode

Guest Mode

Guest Mode uses a wired connection, so people can display content from their devices to the Surface Hub. If the source device is Windows-based, that device can also provide Touchback and Inkback. Surface Hub's internal PC takes video and audio from the connected device and presents them on the Surface Hub. If Surface Hub encounters a High-Bandwidth Digital Content Protection (HDCP) signal, the source is displayed as a black image. To display your content without violating HDCP requirements, use the keypad on the right side of the Surface Hub to directly choose the external source.

> **Tip**
>
> When an HDCP source is connected, use the side keypad to change source inputs.

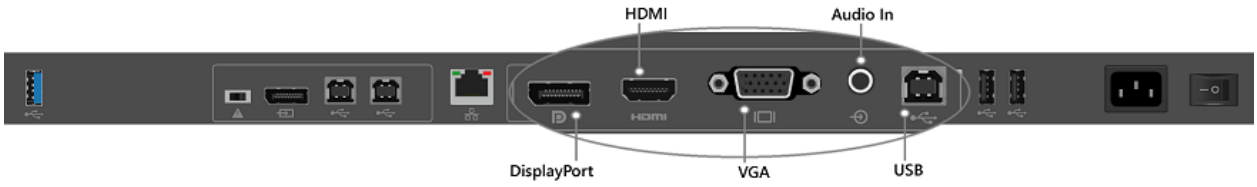
Ports

Use these ports on the Surface Hub for Guest Mode.

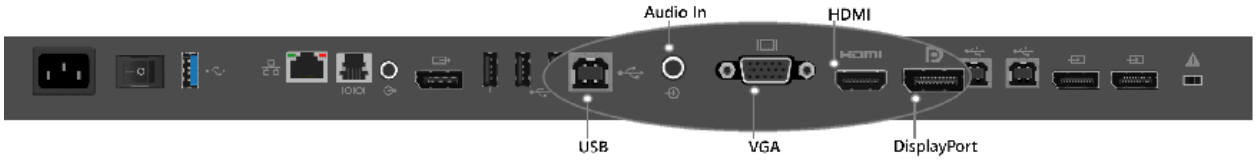
Interface	Type	Description	Capabilities
Display Port 1.1a	Video input	Guest input #1	- Support simultaneous guest input display with guest input #2 and guest input #3 (one full resolution, two thumbnails). - HDCP compliant in bypass mode - Touchback enabled
HDMI 1.4	Video input	Guest input #2	- Support simultaneous guest input display with guest input #1 and guest input #3 (one full resolution, two thumbnails). - HDCP compliant in bypass mode - Touchback enabled
VGA	Video input	Guest input #3	- Support simultaneous guest input display with guest input #1 and guest input #2 (one full resolution, two thumbnails). - HDCP compliant in bypass mode - Touchback enabled
3.5-mm jack	Audio input	Analog audio input	- Ingest into Surface Hub PC, usually with the VGA video input.
USB 2.0, type B	USB out	Touchback	- Provides access to the HID input devices mouse, touch, keyboard, and stylus back to the guest PC.

Port locations

These are the port connections used for Guest Mode on the 55" and 84" Surface Hubs.



Wired port connections on 55" Surface Hub



Wired port connections on 84" Surface Hub

Port enumeration

When a Surface Hub is connected to a guest computer with the wired connect USB port, several USB devices are discovered and configured. These peripheral devices are created for Touchback and Inkback. The peripheral devices can be viewed in Device Manager. Device Manager shows duplicate names for some devices.

Human interface devices

- HID-compliant consumer control device
- HID-compliant pen
- HID-compliant pen (duplicate item)
- HID-compliant pen (duplicate item)
- HID-compliant touch screen
- USB Input Device
- USB Input Device (duplicate item)

Keyboards

- Standard PS/2 keyboard

Mice and other pointing devices

- HID-compliant mouse

Universal serial bus controllers

- Generic USB hub
- USB composite device

Guest Mode connectivity

Your choice of video cable depends on what is available from your source input. The Surface Hub has three choices of video input: DisplayPort, HDMI, and VGA. See the following chart for available resolutions.

Signal Type	Resolution	Frame rate	HDMI - RGB	DisplayPort	VGA
PC	640 x 480	59.94/60	X	X	X
PC	720 x 480	59.94/60	X	X	
PC	1024 x 768	60	X	X	X
HDTV	720p	59.94/60	X	X	X
HDTV	1080p	59.94/60	X	X	X

Source audio is provided by DisplayPort and HDMI cables. If you must use VGA, Surface Hub has an audio input port that uses a 3.5-mm plug. Surface Hub also uses a USB cable that provides Touchback and Inkback from the Surface Hub to compatible Windows 10 or Windows 11 devices. The USB cable can be used with any video input that is already connected with a cable.

Someone using Guest Mode to connect a PC would use one of these options:

- **DisplayPort:** DisplayPort cable and USB 2.0 cable
- **HDMI:** HDMI cable and USB 2.0 cable
- **VGA:** VGA cable, 3.5-mm audio cable, and USB 2.0 cable

If the computer you're using for Guest Mode isn't compatible with Touchback and Inkback, you don't need the USB cable.

Replacement PC Mode

In Replacement PC Mode, the embedded computer of the Surface Hub is turned off and an external PC is connected to the Surface Hub. Connections to replacement PC ports give access to key peripherals on the Surface Hub, including the screen, pen, and touch features. This does mean that your Surface Hub won’t have the benefit of the Windows Team experience, but you'll have the flexibility offered by providing and managing your own Windows computer.

Software requirements

You can run Surface Hub in Replacement PC Mode with 64-bit versions of Windows 10 or Windows 11 Home, Windows 10 or Windows 11 Pro, and Windows 10 or Windows 11

Enterprise. You can download the Surface Hub Replacement PC driver package from the Microsoft Download Center. We recommend that you install these drivers on any computer you plan to use as a replacement PC.

Hardware requirements

Surface Hub is compatible with a range of hardware. Choose the processor and memory confirmation for your replacement PC so that it supports the programs you're using. Your replacement PC hardware needs to support 64-bit versions of Windows 10 or Windows 11.

Graphics adapter

In Replacement PC Mode, Surface Hub supports any graphics adapter that can produce a DisplayPort signal. You improve your experience with a graphics adapter that can match Surface Hub's resolution and refresh rate. For example, the best and recommended replacement PC experience on the Surface Hub is with a 120-Hz video signal.

- **55" Surface Hubs:** For best experience, use a graphics card capable of 1080p resolution at 120 Hz.
- **84" Surface Hubs:** For best experience, use a graphics card capable of outputting four DisplayPort 1.2 streams to produce 2160p at 120 Hz (3840 x 2160 at 120-Hz vertical refresh). Such graphics cards include: NVIDIA Quadro K2200, NVIDIA Quadro K4200, NVIDIA Quadro M6000, AMD FirePro W5100, AMD FirePro W7100, and AMD FirePro W9100.

Check directly with graphics card vendors for the latest drivers.

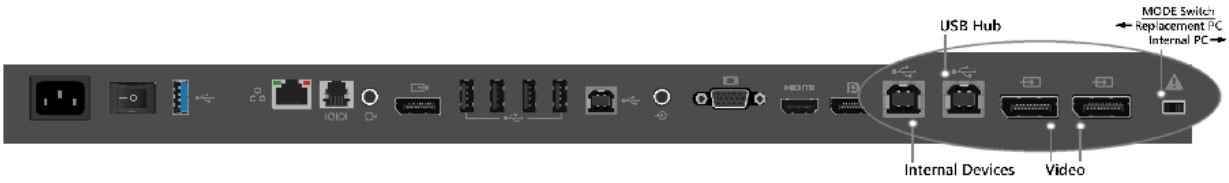
Graphics vendor	Driver download page
NVIDIA	http://nvidia.com/Download/index.aspx
AMD	http://support.amd.com/download
Intel	https://downloadcenter.intel.com/

Replacement PC ports

Replacement PC ports on 55" Surface Hub

Description	Type	Interface	Details
PC video	Video input	DP 1.2	- Full screen display of 1080p at 120 Hz, plus audio - HDCP compliant
Internal peripherals	USB output	USB 2.0 type B	- Touch - Pen - Speakers - Microphone - Cameras - NFC sensor - Ambient light sensor - Passive infrared sensor
USB hub	USB output	USB 2.0 type B	- Underneath USB ports

Replacement PC ports on 84" Surface Hub



Description	Type	Interface	Details
PC video	Video input	DP 1.2 (2x)	- Full screen display of 2160p at 120 Hz, plus audio - HDCP compliant
Internal peripherals	USB output	USB 2.0 type B	- Touch - Pen - Speakers - Microphone - Cameras - NFC sensor - Ambient light sensor - Passive infrared sensor
USB hub	USB output	USB 2.0 type B	- Underneath USB ports

Replacement PC setup instructions

To use Replacement PC Mode

1. Download and install the Surface Hub Replacement PC driver package on the replacement PC.

   > **Tip**
   >
   > Set sleep or hibernation on the replacement PC so the Surface Hub will turn off the display when it isn't being used.

2. Turn off the Surface Hub using the power switch next to the power cable.
3. Connect the cables from the Surface Hub's replacement PC ports to the replacement PC. These ports are usually covered by a removable plastic cover.
   - 55" Surface Hub: Connect one DisplayPort cable and two USB cables.
   - 84" Surface Hub: Connect two DisplayPort cables and two USB cables.
4. Toggle the Mode switch to **Replacement PC**. The Mode switch is next to the Replacement PC ports.
5. Turn on the Surface Hub using the power switch next to the power cable.
6. Press the power button on the right side of the Surface Hub.

You can switch the Surface Hub to use the internal PC.

To switch back to internal PC

1. Turn off the Surface Hub using the power switch next to the power cable.
2. Toggle the Mode switch to Internal PC. The Mode switch is next to the Replacement PC ports.
3. Turn on the Surface Hub using the power switch next to the power cable.

Video Out

The Surface Hub includes a Video Out port for mirroring visual content from the Surface Hub to another display.

Video Out ports

Video Out port on the 55" Surface Hub

Video Out port on the 84" Surface Hub

Description	Type	Interface	Capabilities
Video Output Mirror	Video Output	Video Output	- Supports connection to a standard DisplayPort monitor (only supports an x4 Link displaying 1080p60 resolution at 24 bpp) - Supports use with HDMI monitors (supporting 1080p60) by using a DisplayPort-to-HDMI adaptor

Cables

Both the 55” and 84” Surface Hub devices have been tested to work with Certified DisplayPort and HDMI cables. While vendors do sell longer cables that may work with the Surface Hub, only those cables that have been certified by testing labs are certain to work with the Hub. For example, DisplayPort cables are certified only up to 3 meters, however many vendors sell cables that are three times that length. If a long cable is necessary, we strongly suggest using HDMI. HDMI has many cost-effective solutions for long-haul cables, including the use of repeaters. Nearly every DisplayPort source automatically switches to HDMI signaling if an HDMI sink is detected.

Bluetooth accessories

You can connect the following accessories to Surface Hub using Bluetooth:

- Mice
- Keyboards
- Headsets

- Speakers

> **Tip**
>
> After you connect a Bluetooth headset or speaker, you might need to change the **default microphone and speaker settings**.

Miracast over infrastructure

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

Miracast over Infrastructure offers many benefits:

- Windows automatically detects when sending the video stream over this path is applicable.
- Windows will only choose this route if the connection is over Ethernet or a secure Wi-Fi network.
- Users don't have to change how they connect to a Miracast receiver. They use the same UX as for standard Miracast connections.
- No changes to current wireless drivers or PC hardware are required.
- It works well with older wireless hardware that isn't optimized for Miracast over Wi-Fi Direct.
- It uses an existing connection, which reduces the time to connect and provides a stable stream.

How it works

Users attempt to connect to a Miracast receiver through their Wi-Fi adapter. When the list of Miracast receivers is populated, Windows identifies that the receiver is capable of supporting a connection over the infrastructure. When the user selects a Miracast receiver, Windows attempts to resolve the device's hostname via standard DNS, and via multicast DNS (mDNS). If the name isn't resolvable via either DNS method, Windows falls back to establishing the Miracast session using the standard Wi-Fi direct connection.

> **Tip**
>
> For more information on the connection negotiation sequence, see **Miracast over Infrastructure Connection Establishment Protocol (MS-MICE)**

Enabling Miracast over Infrastructure

If you have a Surface Hub or other Windows 10/11 device, then you automatically have this new feature. To take advantage of it in your environment, you need to ensure the following is true within your deployment:

- Open TCP port: **7250**.

- A Surface Hub or Windows PC can act as a Miracast over Infrastructure *receiver*. A Windows PC or phone can act as a Miracast over Infrastructure *source*.
  - As a Miracast receiver, the Surface Hub or device must be connected to your enterprise network via either Ethernet or a secure Wi-Fi connection (for example, using either WPA2-PSK or WPA2-Enterprise security). If the Surface Hub or device is connected to an open Wi-Fi connection, Miracast over Infrastructure will disable itself.
    - As a Miracast source, the Windows PC or phone must be connected to the same enterprise network via Ethernet or a secure Wi-Fi connection.
- The DNS Hostname (device name) of the Surface Hub or device needs to be resolvable via your DNS servers. You can achieve this by either allowing your Surface Hub to register automatically via Dynamic DNS, or by manually creating an A or AAAA record for the Surface Hub's hostname.
- Windows 10 PCs must be connected to the same enterprise network via Ethernet or a secure Wi-Fi connection.

It's important to note that Miracast over Infrastructure isn't a replacement for standard Miracast. Instead, the functionality is complementary, and provides an advantage to users who are part of the enterprise network. Users who are guests to a particular location and don’t have access to the enterprise network will continue to connect using the Wi-Fi Direct connection method.

The **InBoxApps/WirelessProjection/PinRequired** setting in the SurfaceHub configuration service provider (CSP) isn't required for Miracast over Infrastructure. This is because Miracast over Infrastructure only works when both devices are connected to the same enterprise network. This removes the security restriction that was previously missing from Miracast. We recommend that you continue using this setting (if you used it previously) as Miracast will fall back to regular Miracast if the infrastructure connection doesn't work.

Learn more

- Troubleshoot display projection to Surface Hub

Troubleshoot display projection to Surface Hub

Article • 02/16/2023

Surface Hub is designed to enable end users to project their display from laptops or other external devices wirelessly via Miracast or via wired (USB-C/HDMI) connections. Surface Hub listens for incoming wireless connections via Miracast when Wi-Fi is enabled. If your external device supports Miracast and runs Windows 10 or Windows 11, you should be able to wirelessly project your screen onto Surface Hub. If you can't, try the troubleshooting steps on this page.

To connect with Miracast:

1. On your Windows 10/11 device, press **the Windows logo key + K**.
2. In the **Connect** window, look for the name of your Surface Hub in the list of nearby devices, as shown in the bottom left corner of the Surface Hub display.
3. Enter a PIN if your system administrator has enabled the PIN setting for Miracast connections. This requires you to enter a PIN when you connect to Surface Hub for the first time.

> **Tip**
>
> If you don’t see the name of the Surface Hub device as expected, it's possible the previous session was prematurely closed. If so, sign in to Surface Hub directly to end the previous session and connect from your external device.

Troubleshoot Miracast

Table 1. Troubleshoot Miracast connections to Surface Hub

Action	Where	Notes
Restart devices	External device/Surface Hub	If Miracast has worked previously, restart your external device or restart your external device and Surface Hub to reset the connection.
Restart wireless display adapter	External device	1. **Start** > **Settings** > Bluetooth **& devices** > **Devices**. Under **Wireless displays & docks**, select the wireless display or adapter. 2. Select **Remove device** > **Yes**. 3. Try reconnecting.

Action	Where	Notes
Check Wi-Fi is turned on	Surface Hub	- Open **Settings** > **View as Admin**. Select **Network & Internet** and make sure **Wi-Fi** is turned **On**. **Note**: Surface Hub doesn't need to be connected to a wireless network, but Wi-Fi must be enabled for Miracast to work.
Verify Miracast projection is turned on	Surface Hub	1. Open **Settings** > **View as Admin**. Select Surface Hub> Projection. 2. Make sure the following settings are turned on: - **Connect automatically when someone projects** - **Presenters can use Miracast to protect wirelessly to this device** **Note:** If a PIN is required, users must enter it when they connect an external device for the first time.
Verify Miracast support	External device	1. Press **Windows logo key** + **R** and type **dxdiag**. 2. Select **Save all information.** 3. Open the saved **dxdiag.txt** file and find **Miracast**. It should indicate **Available, with HDCP**.
Check Miracast channel	Surface Hub	If you run a network scan, you should see Surface Hub Miracast listed as an access point. If Surface Hub's Miracast network appears, but you can't see it as an available device, try to adjust the Miracast channel. When Surface Hub is connected to a Wi-Fi network, it uses 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'll need to restart Surface Hub after each change. Use channels that don't show heavy utilization from the network scan.
Check drivers	External device	Ensure the device drivers on your external device are up to date and the latest firmware is installed for your wireless display or adapter. In **Device Manager**, select **Network Adapters**, open the Wi-Fi adapter and video adapter and check for an updated driver version.
Check firewall	External device	The Windows firewall can block Miracast traffic. The most straightforward 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.

Action	Where	Notes
Check Group Policy settings	External device (domain joined)	On domain-joined devices only, Group Policy can also block Miracast. 1. Press **Windows Key + R** and type **rsop.msc.** The **Resultant Set of Policy** snap-in shows the current policy settings applied to the PC. 2. Review **Computer Configuration** > **Windows Settings** > **Security Settings** > **Wireless Network (IEEE 802.11) Policies**. There should be a setting for wireless policies. 3. Double-click the setting for wireless policies, and a dialog box appears. 4. Open the **Network Permissions** tab and select **Allow everyone to create all user profiles**.
Check Event logs	External device/Surface Hub	The last place to check is in the Event logs. Miracast events are logged to **Wlanautoconfig** on both Surface Hub and the external device. If you export Surface Hub logs, you can view Surface Hub's Wlanautoconfig in the **WindowsEventLog** folder. The event log errors can provide more details on where the connection fails.

Troubleshoot connection performance

After wireless projection is connected, it's 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 use channels with less traffic.

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

If Surface Hub and the projecting device are connected to Wi-Fi but use different access points with different channels, forced channel switching degrades performance when Miracast is connected. The channel switching affects 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 Surface Hub's channel 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. Some channel switching is unavoidable if there are multiple Wi-Fi networks or access points in the environment. In this scenario, ensure all Wi-Fi drivers are up to date.

Surface Hub Miracast channels 149-165 not supported in Europe, Japan, Israel

In compliance with regional governmental regulations, all 5-GHz wireless devices in Europe, Japan, and Israel don't support the Unlicensed National Information Infrastructure-3 (U-NII-3) band. In Surface Hub, the channels associated with U-NII-3 are 149 through 165. This includes Miracast connections on these channels. Therefore, Surface Hubs used in Europe, Japan, and Israel can't use channels 149-165 for Miracast connections.

Troubleshoot wired connections

- Device resolution not supported error
- Connect app exits unexpectedly

Device resolution not supported error

When you try to project from a Surface Pro, Surface Book, or Surface Laptop to an 84-inch Surface Hub by using the HDMI port on the Surface Hub, the error message "Device Resolution isn't supported" is displayed.

- **Cause:** The Surface device isn't set to a supported 84" ingest resolution. By default, Windows tries to connect to the Surface Hub using *Duplicate* mode, duplicating your desktop on both screens. But the default resolution of the Surface device is higher than the 1080-p resolution of the Surface Hub, so the Hub can't display the higher-resolution image.
- **Resolution:** Projecting to a second screen can be accomplished by using *Extend*. Extend is used to expand the desktop user interface across your Surface and Surface Hub displays, allowing each to display the desktop in its native resolution. Use one of the following methods to configure your Surface to display your desktop in Extend mode.

Method 1: Change the desktop resolution

1. Open **Start**, and then select **Settings** > **System** > **Display**.
2. Select the Surface Hub display from the choice made available.
3. Under **Scale and layout**, change the setting under **Resolution** to **1920 x 1080**.

Method 2: Change Project setting to Extend

- Press **Windows key+P** and then select **Extend**.

Connect app exits unexpectedly

At times, a wired Connect session that is started from the Welcome screen by connecting a DisplayPort input will exit back to the Welcome screen after using the side keypad or the source button to cycle through all source inputs.

- **Cause:** This is an issue in the Connect app and its default full-screen state. By changing the size of the app or by selecting a DisplayPort input thumbnail in the Connect app, you can prevent input cycling from affecting the app.
- **Resolution:** Launch the Connect app from the Welcome screen and connect a DisplayPort input to resolve this issue. If the input is already connected, manually select the thumbnail.

Contact Support

If you have questions or need help, you can create a support request.

Learn more

- Connect devices to Surface Hub 2S
- Connect other devices and display with Surface Hub v1

Microsoft Teams Rooms on Surface Hub

Article • 04/11/2023

Teams Rooms for Surface Hub automatically replaces the previous Surface Hub Teams app upon installation of KB5004196, KB5004198, and KB5004199 that released on September 30, 2021.

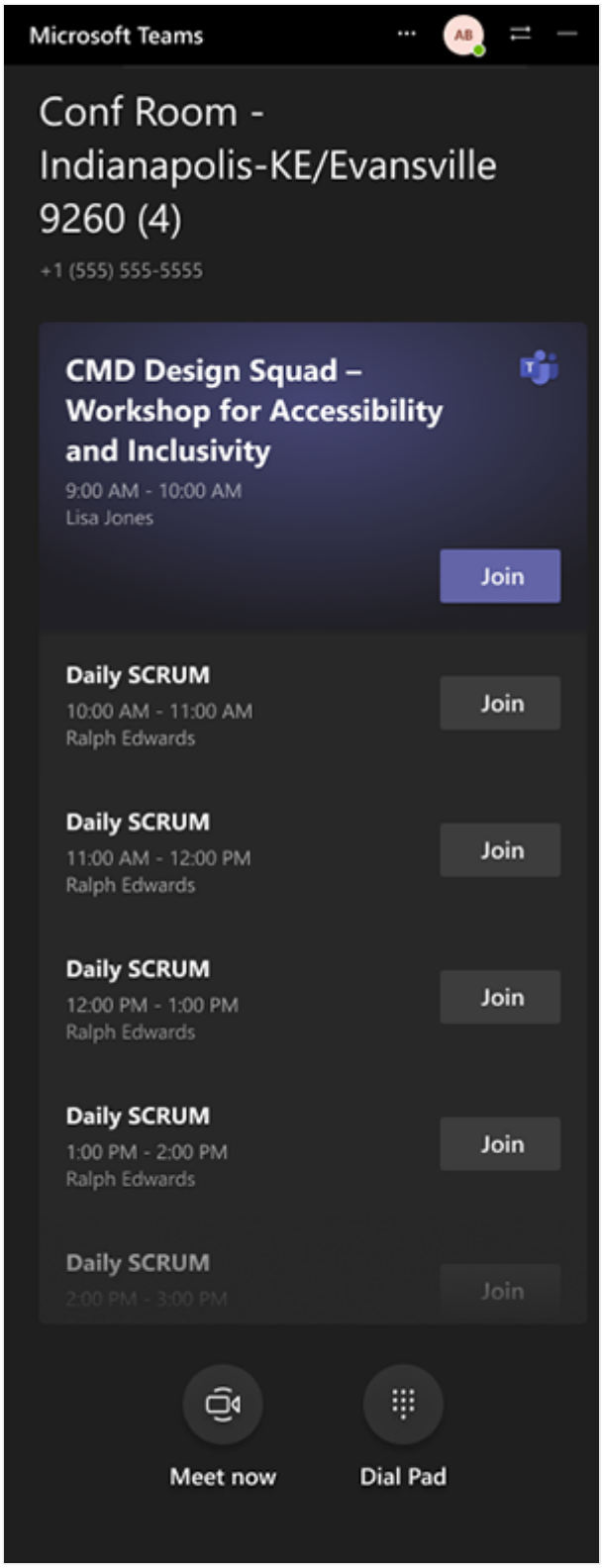
What's new?

- Meetings joined from the Surface Hub Welcome Screen or new Agenda page are joining "Edge to Edge" to put people in the foreground.
- Familiar meeting features including chat bubbles, reactions, desktop and application sharing, give and take control and audio, full PowerPoint live support, together mode, and large gallery.
- Teams Rooms on Surface Hub can run side by side with other applications or run minimized.
- Admins can configure features like Coordinated Meeting, Proximity Join for Surface Hub, and Direct Guest Join. XML files are supported and will be migrated to the new settings model.
- New QoS Options and network requirements. To learn more, see Configure networking and Quality of Service for Microsoft Teams Rooms on Surface Hub.
- If it is not already the default, Teams can be set as the default app for meetings and calls in **Settings** > **Surface Hub** > **Calling & audio**. To learn more about meeting modes and configuring them through MDM policy, see Manage Surface Hub with an MDM provider.

> **Tip**
>
> As a companion to this article, we recommend using the **Surface Hub and Microsoft Teams Rooms automated setup guide** when signed in to the Microsoft 365 Admin Center. This guide will customize your experience based on your environment. If you're hosted in Exchange Online and using Microsoft Teams, the guide will automatically create your device account with the correct settings. Or use it to validate existing resource accounts to help turn them into compatible Surface Hub device accounts. To review best practices without signing in and activating automated setup features, go to the **M365 Setup portal**.

In meeting experience

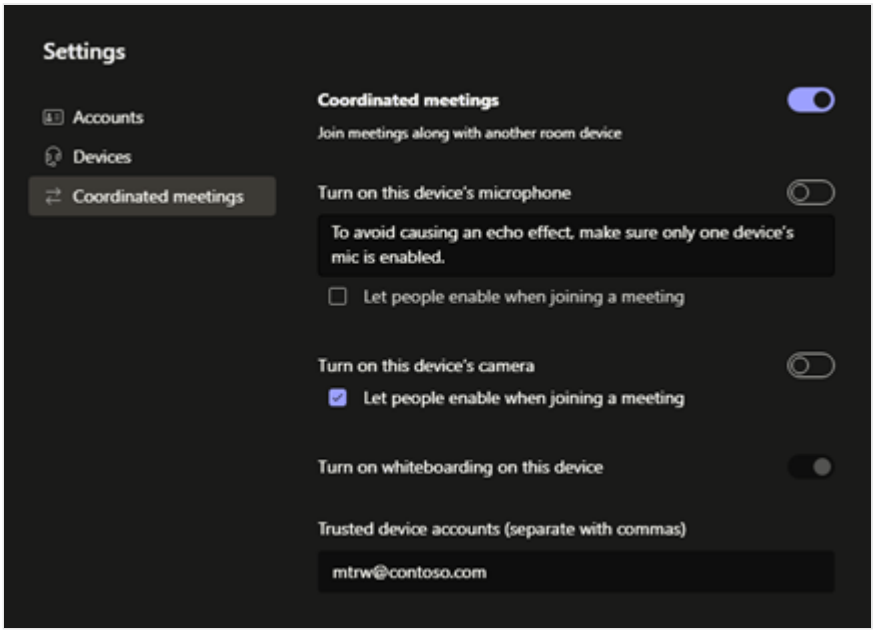
Teams Rooms on Surface Hub Meetings experience are aligned to the familiar experience that users know from their personal devices with adjustments made to optimize for a large screen device. Opening Teams on Surface Hub lets users access key features including One-touch meeting join, Meet Now and Dial Pad for PSTN or peer-to-peer calls.



Manage Teams Rooms on Surface Hub

You can customize the Teams experience directly from the Settings menu after entering administrative credentials, including:

- Configure Coordinated Meetings and Proximity join.
- Adjust settings for default microphones, cameras, and speakers.
- Check the client version and search for the latest updates.



The new Teams Rooms for Surface Hub client, will automatically apply existing settings configured via XML files, provisioning packages, or an MDM provider. These methods, explained in Manage Microsoft Teams configuration on Surface Hub, will be superseded by new cloud-based solutions, as described below in Simplified management of Teams coming to Surface Hub.

Prepare networking for Teams Rooms

To optimize Teams Rooms, refer to the requirements and recommendations described in Configure networking and Quality of Service for Microsoft Teams Rooms on Surface Hub.

Simplified management of Teams on Surface Hub

- **Teams Admin Center.** Teams Admin Center provides a comprehensive self-management platform to monitor and manage the Teams Rooms experience on Teams devices. Teams Admin Center is available to Microsoft Teams Rooms users at no additional cost.
- **Microsoft Teams Rooms managed service.** The Microsoft Teams Rooms managed service is a cloud-based IT management and monitoring service that keeps Microsoft Teams Rooms devices and their peripherals up to date and proactively monitored, supporting an environment optimized for a great user experience.

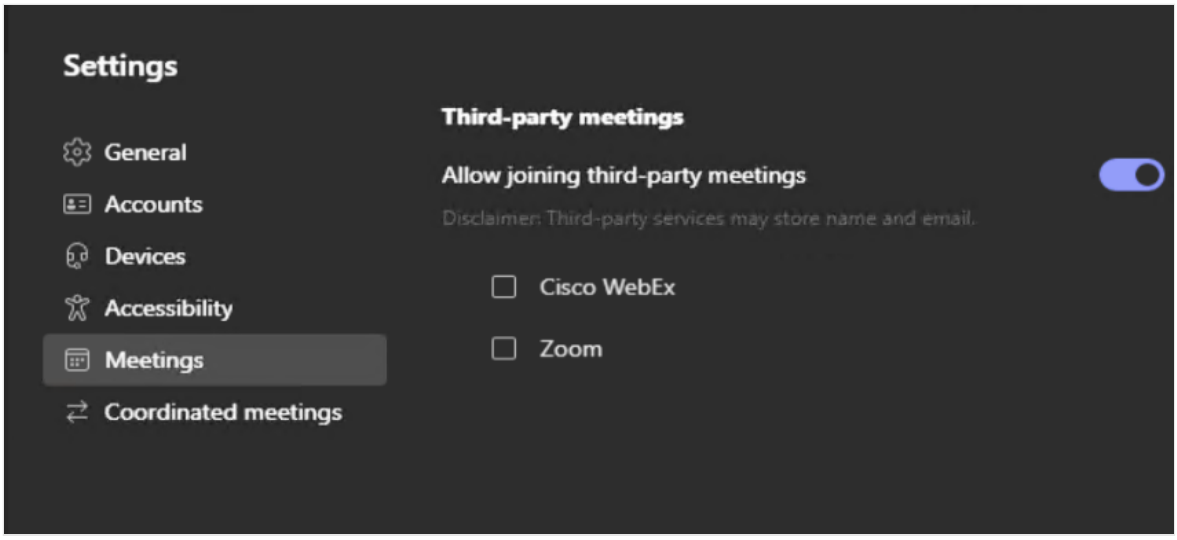
Third-party meetings on Surface Hub

Microsoft Teams Rooms on Surface Hub supports joining third-party online meetings, referred to as Direct Guest Join. You can use Surface Hub to join meetings hosted on Cisco Webex and Zoom. And others can join Teams meetings on Hub from their third-party room systems. This feature is rolling out to Surface Hubs beginning October 5, 2022.

To enable third-party meetings on Surface Hub

1. Open Teams, select Settings (...), and enter your admin username and password.

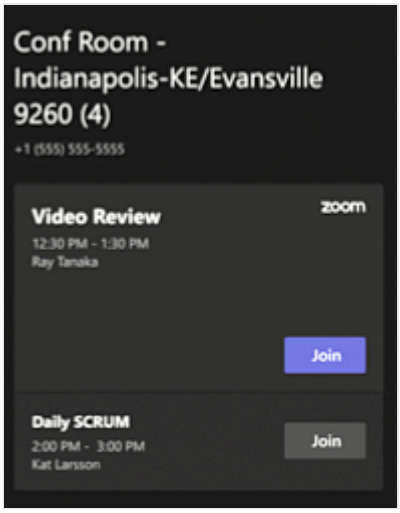
2. Select **Meetings** and then select **Allow joining third-party meetings**.



3. Select **Cisco WebEx** or **Zoom**, as appropriate.

To join third-party meetings

1. Select **Home**, select the meeting tile from the home screen calendar, or go directly to the Teams agenda page, which includes join buttons for the third-party-enabled meetings.



2. Select **Join**. When the Microsoft Edge browser launches you into the meeting, you'll need to allow the browser to use the Surface Hub microphone and camera for the meeting.

> ⓘ Note
>
> Microphone and camera approvals are removed when you end a Surface Hub session, and you will be asked to allow them again in the next session.

3. Enter your name and other required fields to start the meeting.

Optional advanced configuration for third-party meetings

Depending on your environment, you may need to configure more settings. For example, you should ensure your organization has no policies preventing you from connecting to third-party meeting services.

Configure Edge policy settings

To enable a more seamless experience that avoids users having to approve the microphone and camera for each Hub session, you can configure the following Edge policies via Microsoft Intune admin center. To learn more, see Create a device profile in Microsoft Intune.

Microsoft Edge policy setting	Location	Notes
Force synchronization of browser data and do not show the sync consent prompt	Devices > Configuration Profiles > Administrative Templates > Edge Chromium General Policies > Properties	Set to **Enable**
Sites that can access video capture devices without requesting permission	Devices > Configuration Profiles > Administrative Templates > Edge Chromium General Policies > Properties	Prevents camera approval prompt. Add https://www.zoom.com or https://www.webex.com as appropriate.
Sites that can access audio capture devices without requesting permission	Devices > Configuration Profiles > Administrative Templates > Edge Chromium General Policies > Properties	Prevents audio approval prompt. Add https://www.zoom.com or https://www.webex.com as appropriate.
Default geolocation setting	Devices > Configuration Profiles > Administrative Templates > Edge Chromium General Policies > Properties	Prevents geolocation prompt, if desired. If you wish to prevent third-party meetings from tracking the location of your Surface Hub, set **BlockGeolocation (2)**. If you don't configure this setting, users will be prompted to allow Zoom or Webex to track the location of Surface Hub.

Optionally, you may wish to configure calendar processing rules to enable "auto accept," "auto decline," and related settings.

To learn more, see Enable Teams Rooms devices to join third-party meetings and related Teams Rooms documentation.

Support for Teams Rooms in Government Community Cloud High (GCC-H)

A one-time manual update of the Teams Rooms client to version 1.4.00.25354 is needed in order to for it to be able to connect to a GCC-H tenant and then keep itself up-to-date automatically:

- Confirm that your Hub has KB5005611 or a later Windows Cumulative Update installed
- Use Teams_Uninstall_win32.ppkg to remove current Teams Rooms on Surface Hub version
- Restart your device
- Install Teams_win32.ppkg to install version 1.4.00.25354
- Restart your device again

Detailed steps:

1. Save both provisioning packages to the root of your USB drive.
2. Insert the USB drive into your Surface Hub.
3. On your Surface Hub, open the Start menu, select All apps, and then select Settings.
4. Provide your Hub admin credentials when prompted.
5. Go to **Surface Hub** > **Device management** > **Add or remove a provisioning package**, and then select **Add a package**.
6. Under **Select a package**, select the Teams_Uninstall_win32.ppkg provisioning package, and then restart your Surface Hub.
7. On your Surface Hub, open the Start menu, select All apps, and then select Settings.
8. Provide your Hub admin credentials when prompted.
9. Go to **Surface Hub** > **Device management** > **Add or remove a provisioning package**, and then select **Add a package**.
10. Under **Select a package**, select the Teams_win32.ppkg provisioning package, and then restart your Surface Hub.

Learn more

- Surface Hub and Microsoft Teams Rooms automated setup guide

Configure networking and Quality of Service for Microsoft Teams Rooms on Surface Hub

Article • 01/27/2023

This article explains how to prepare your environment to optimize Microsoft Teams Rooms on Surface Hub.

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 Create and test a device account

Check network availability

> **Tip**
>
> As a companion to this article, we recommend using the **Surface Hub and Microsoft Teams Rooms automated setup guide** when signed in to the Microsoft 365 Admin Center. This guide will customize your experience based on your environment. If you're hosted in Exchange Online and using Microsoft Teams, the guide will automatically create your device account with the correct settings. Or use it to validate existing resource accounts to help turn them into compatible Surface Hub device accounts. To review best practices without signing in and activating automated setup features, go to the **M365 Setup portal**.

Teams Rooms on Surface Hub must have access to a network that meets these requirements:

- Access to your Active Directory or Azure Active Directory (Azure AD) instance
- Access to a server that can provide an IP address using DHCP. Microsoft Teams Rooms on Surface Hub 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 Microsoft 365 and Microsoft 365 URLs and IP address ranges for Microsoft Teams.

> **Important**
>
> Microsoft Teams Rooms does not support proxy authentication as it may interfere with regular operations of Teams. Ensure that Surface Hub devices or Microsoft 365 service endpoints have been exempted from proxy authentication before going into production with Teams Rooms on Surface Hub.

Implement Quality of Service (QoS) on Surface Hub

Quality of Service (QoS) is a combination of network technologies that allows the administrators to optimize the experience of real time audio/video and application sharing communications. Configuring QoS for Microsoft Teams on the Surface Hub can be done using your mobile device management (MDM) provider or through a provisioning package.

To configure QoS for Surface Hub using Microsoft Intune:

1. In Intune, create a custom policy.

2. In **Custom OMA-URI Settings**, select **Add**. For each setting that you add, you will enter a name, description (optional), data type, OMA-URI, and value.

3. To ensure optimal video and audio quality on Surface Hub, add the following QoS settings to the device.

Name	Description	OMA-URI	Type	Value
Audio Ports	Audio Port range	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsAudio/SourcePortMatchCondition	String	50000-50019
Audio DSCP	Audio ports marking	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsAudio/DSCPAction	Integer	46
Video Port	Video Port range	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsVideo/SourcePortMatchCondition	String	50020-50039
Video DSCP	Video ports marking	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsVideo/DSCPAction	Integer	34
Sharing Port	Sharing Port range	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsSharing/SourcePortMatchCondition	String	50040-50059
Sharing DSCP	Sharing ports marking	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsSharing/DSCPAction	Integer	18

4. When the policy has been created, deploy it to Surface Hub.

Learn more

- Surface Hub and Microsoft Teams Rooms automated setup guide
- Microsoft 365 network connectivity principles
- Implement Quality of Service (QoS) in Microsoft Teams

Microsoft Teams app for Surface Hub

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

The Microsoft Teams app for Surface Hub is periodically updated and available via the Microsoft Store. If you manage Surface Hub with Automatic Updates enabled (default setting), the app will update automatically.

Version history

Store app version	Updates	Published to Microsoft Store
0.2020.84.19701	- Coordinated Teams meetings with Microsoft Teams Rooms - Proximity-based meeting join	August 12, 2020
0.2020.521.2344.0	- 3x3 Gallery view on Surface Hub - Ability to search for External users	June 10, 2020
0.2020.13201	- Quality improvements and Bug fixes	June 1, 2020
0.2020.4301.0	- Accept incoming PSTN calls on Surface Hub - Consume Attendee/Presenter role changes	May 21, 2020

Learn more

- Manage Microsoft Teams settings on Surface Hub

Troubleshoot Teams sign-in issues on Surface Hub

Article • 01/25/2023

If you can't sign in to Microsoft Teams on Surface Hub, several recommended troubleshooting steps are described on this page.

- First, make sure your Surface Hub is running the latest updates. To learn more, see the following video: How to verify a Surface Hub is fully updated .
- Check Microsoft Teams is updated to the latest version. On Surface Hub, open **Microsoft Teams**, select **...** > **Settings** > **Check for updates**.
- Use the Azure sign-in logs for insights into sign-in errors. You can filter by the Surface Hub device account and look for any failures.
- If you still can't sign in, look for the error code displayed on the Teams sign-in screen and review the following table for troubleshooting steps and links to relevant documentation.

Error codes	Possible root cause	How to resolve	Learn more
CAA20003	Incorrect time on device	Ensure KB5011543 or a newer Windows update is installed (build 19042.1682 or later).	- Video: How to verify a Surface Hub is fully updated - Manage Windows updates on Surface Hub

Error codes	Possible root cause	How to resolve	Learn more
	Conditional Access (CA) Policy	A device account can't have CA enabled. To resolve this issue, ensure your Surface Hub device account is excluded from any CA policies. 1. Begin with the Azure AD conditional access What If tool to see which policies currently apply to your device account. 2. Run the tool in Report-only mode, which lets you evaluate the impact of Conditional Access policies before enabling them in their environment.	- Troubleshooting sign-in problems with Conditional Access - Troubleshoot Conditional Access using the What If tool - What is Conditional Access report-only mode? - Video: Use the Report Only feature to test Conditional Access policies
CAA90014	Device account password expired	1. Open Microsoft Edge and attempt to sign in to Microsoft 365 with your device account credentials. 2. If prompted to change the device account password, go ahead and change it. 3. On Surface Hub, go to **Settings** > **Surface Hub** > **Accounts**> **Device account** > **Change**. 4. Select **Start over with a new device account**. The current device account will be removed when you set up a new one using your new credentials.	- Password management (Surface Hub)
	Incorrect time on device	Ensure KB5011543 or a newer Windows update is installed (build 19042.1682 or later).	- Video: How to verify a Surface Hub is fully updated - Manage Windows updates on Surface Hub

Error codes	Possible root cause	How to resolve	Learn more
	Multi-Factor Authentication (MFA)	A device account can't have MFA enabled. To resolve this issue, try excluding the Surface Hub device account from MFA and test again.	- Create and test a device account
CAA10001 or AUTH0006	Conditional Access (CA) Policy	Follow the instructions above to resolve Conditional Access issues.	
	No device account added	To confirm a device account is added: 1. On Surface Hub, go to **Settings** > **Surface Hub** > **Accounts**. 2. Verify that a device account is added successfully: A device account will show as **Not Set** if it isn't added. 3. Create and add a device account and try connecting to Teams again.	- Create and test a device account
unknownautherror	Hub still running earlier OS	Surface Hub v1 only: 1. Ensure the device is updated to Windows 10 Team 2020 Update (20H2). 2. If your Hub v1 device is still running an earlier OS, it could be affected by the following known issue: **A small subset of v1 Surface Hub devices is not able to automatically upgrade to the Windows 10 Team 2020** 3. To resolve, reimage Hub v1 using the Surface Hub Recovery Tool and upgrade to 20H2.	- Known issues: Surface Hub - Using the Surface Hub Recovery Tool
	Conditional Access (CA) Policy	Follow the instructions above to resolve Conditional Access issues.	

Support requests

If you still can't successfully sign in to Teams, you can create a support request. Include the following items:

- Any error codes displayed when you attempt to sign in to Teams.
- Log files, as noted below.

Diagnostic Teams log files

When creating a support request with Microsoft Support, the support engineer will require diagnostic log files. Having the logs before creating the support request will allow Microsoft to quickly start troubleshooting the problem.

To collect Teams log files:

1. Connect an external keyboard to Surface Hub.
2. Open the Teams app and reproduce the issue by attempting to sign in.
3. Select the Teams app and ensure the focus is on Teams as the active app on the Hub display.
4. On your keyboard, press **Tab** three times to highlight the UI element for settings, represented by three dots (**...**).
5. Press **CTRL + ALT + SHIFT + 1** to download the Teams log files.
6. Open **File Explorer**, go to **Downloads**, and look for the folder containing the Teams log files.
7. Copy the folder to a USB drive.

To learn more, see Configure log files for monitoring and troubleshooting in Teams

Surface Hub & Azure log files

- Surface Hub log files
- Any applicable Azure sign-in logs that indicate sign-in failure

Create and configure resource accounts for rooms and shared Teams devices

Article • 05/04/2023

This article provides steps to create resource accounts for shared spaces and devices, and it includes steps to configure resource accounts for Microsoft Teams Rooms on Windows, Teams Rooms on Android, Teams Rooms on Surface Hub, and hot-desking on Teams displays.

Microsoft 365 resource accounts are mailbox and Teams accounts that are dedicated to specific resources, such as a room or projector. These resource accounts can automatically respond to meeting invites using rules you define when they're created. For example, if you have a common resource such as a conference room, you can set up a resource account for that conference room that will automatically accept or decline meeting invites depending on its calendar availability.

Every resource account is unique to a single Microsoft Teams Rooms installation or Teams display hot-desking implementation.

> **ⓘ Important**
>
> Microsoft 365 resource accounts aren't the same as Teams resource accounts. Teams resource accounts can be used with call queues and auto attendants to accept phone calls from external phone numbers. Microsoft 365 resource accounts are tied to an Exchange Online mailbox and enable booking of shared resources, such as rooms, projectors, and so on.
>
> If you want to know more about Teams resource accounts, see **Manage resources accounts in Microsoft Teams**.

> **ⓘ Note**
>
> If using Microsoft Teams panels, the Teams Rooms resource account signs in to both Teams Rooms and associated Teams panels.

> **ⓘ Note**
>
> **Skype for Business**

If you need to enable your resource account to work with Skype for Business, see **Deploy Microsoft Teams Rooms with Skype for Business Server**

Before you begin

Requirements

Depending on your environment, you need one or more roles to create resource accounts.

Environment	Required Roles
Azure Active Directory	Global Administrator or User Administrator
Active Directory	Active Directory Enterprise Admins, Domain Admins, or have delegated rights to create users. Azure Active Directory Connect Sync rights.
Exchange Online	Global Administrator or Exchange Administrator
Exchange Server	Exchange Organization Management or Recipient Management

ⓘ Important

If you're creating resource accounts for Teams Rooms, the resource account's UPN must match the SMTP address of the resource account.

What license do you need?

In the next step you'll create a resource account for your Teams Rooms console. Before you do that, you need to purchase a license because each resource account you want to associate with a Teams Rooms console needs a Teams Rooms license.

Follow the steps below to purchase a Teams Room Basic or Teams Rooms Pro license that you can assign to a resource account in a later step. For a comparison between the Teams Rooms Basic and Teams Rooms Pro licenses, see Teams Meeting Room Licensing Update.

ⓘ Note

If you have multiple Teams Rooms consoles, we recommend that you purchase a Teams Rooms Pro license for each of your consoles. The Teams Rooms Pro license enables more advanced remote management and analytics for Teams Rooms, enabling you to create a more consistent and robust Teams Rooms and meeting experience.

1. Go to the Microsoft 365 admin center and log in with an account that has global admin permissions.
2. In the admin center, go to the **Billing** > Purchase services page.
3. On the **Purchase services** page, type in **Teams Rooms** in the search box and press enter.
4. Select **Details** under either **Teams Rooms Basic** or **Teams Rooms Pro**.
5. Select the number of licenses you want to purchase in **Select license quantity**.
6. Select how often you want to be billed under **Select billing frequency** and then click **Buy**.

> **Note**
>
> You can purchase up to 25 Teams Rooms Basic licenses. Any additional licenses you purchase beyond 25 must be Teams Rooms Pro licenses.
>
> You can purchase a Teams Rooms Basic license for a Teams Room console and later change the license for that console to Teams Rooms Pro. First make sure you have an available Teams Rooms Pro license and then follow the instructions in **Change the apps and services a user has access to**.

Create a resource account

Each Microsoft Teams Rooms device needs its own resource account. The resource account is the account the Teams Rooms device logs into and is what users in your organization invite to book the Teams Room.

When you create the resource mailbox, you can specify whether you want to allow recurring meetings, have the room auto accept invites, how many days into the future to accept invites, and so on.

> **Tip**
>
> When naming your resource accounts, we recommend using a standard naming convention to the beginning of the e-mail address. This will help with creating

dynamic groups to ease management in Azure Active Directory. For example, you could use "mtr-" for all resource accounts that will be associated with Microsoft Teams Rooms.

Tip

We recommend that you create all resource accounts using Exchange Online and Azure Active Directory.

You can automatically configure recommended Teams Rooms resource settings via the **Surface Hub and Microsoft Teams Rooms automated setup guide**.

Create a resource account using a method from one of the following tabs:

In Microsoft 365 admin center

1. Sign in to the Microsoft 365 admin center.
2. Provide the admin credentials for your Microsoft 365 tenant.
3. Go to **Resources** in the left panel, and then select **Rooms & equipment**. If these options aren't available in the left panel, you may need to select **Show all** first.
4. Select **Add resource** to create a new resource account. Enter a display name and email address for the account and then select **Save**.
5. By default, resource accounts are configured with the following settings:

   - Allow repeat meetings
   - Automatically decline meetings outside of the following limits
     - Booking window (days): 180
     - Maximum duration (hours): 24
   - Auto accept meeting requests

   If you want to change them, select **Edit booking options** before you select **Close**. If you want to change them later, go to **Resources** > **Rooms & equipment**, select the resource account. Then under **Booking options**, select **Edit**.
6. Go to **Users** > **Active users**, and select the room you created to open the properties panel.

7. Next, assign a password to the resource account. In the panel, select **Reset password**.

8. Requiring users to change the password on a shared device will cause sign in problems. Uncheck **Require this user to change their password when they first sign in**, and select **Reset password**.

You may also need to apply bandwidth policies or meeting policies to this account. You can set mailbox policies in a later step.

> **ⓘ Important**
>
> If you're only using this resource account to book space and automatically accept or decline invitations, you've completed the set up. If you're using this resource account for PSTN calling, see **Microsoft Teams add-on licenses** to determine what license it needs.

Configure mailbox properties

You can improve your Teams Rooms meeting experience by customizing how the resource account responds to, and processes, meeting invitations. Using Exchange Online PowerShell, you can set the following resource account properties:

- **AutomateProcessing:** `AutoAccept` Meeting organizers receive the room reservation decision directly without human intervention.
- **AddOrganizerToSubject:** `$false` The meeting organizer isn't added to the subject of the meeting request.
- **DeleteComments:** `$false` Keep any text in the message body of incoming meeting requests. This is required to process external Teams and third-party meetings to provide One Touch Join experience.
- **DeleteSubject:** `$false` Keep the subject of incoming meeting requests.
- **ProcessExternalMeetingMessages:** `$true` Specifies whether to process meeting requests that originate outside the Exchange organization. Required for external Teams meetings and third-party meetings.
- **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 Microsoft Teams Meeting room!"** The additional text to add to the meeting acceptance response.

To configure these properties, you need to connect to Exchange Online PowerShell. For more information, see Connect to Exchange Online PowerShell.

After you've connected to Exchange Online PowerShell, you can configure the mailbox properties on a resource account by using the Set-CalendarProcessing cmdlet.

The following example sets the properties for the `ConferenceRoom01` resource account:

PowerShell

```
Set-CalendarProcessing -Identity "ConferenceRoom01" -AutomateProcessing
AutoAccept -AddOrganizerToSubject $false -DeleteComments $false -
DeleteSubject $false -ProcessExternalMeetingMessages $true -
RemovePrivateProperty $false -AddAdditionalResponse $true -
AdditionalResponse "This is a Microsoft Teams Meeting room!"
```

Turn off password expiration

Like any Microsoft 365 account, a newly-created resource account's password is set to expire automatically after a period of time. However, if the resource account password expires, the Teams Rooms device it's signed into won't be able to sign in again the expiration date.

To avoid having to reset the resource account's password and then logging into each Teams Rooms device again, you can turn off password expiration for the account.

> ⓘ **Note**
>
> Setting **Password never expires** is a requirement for shared Microsoft Teams devices. If your domain rules prohibit passwords that don't expire, you'll need to create an exception for each Teams device resource account.

Follow the steps in one of the following tabs to turn off password expiration:

Microsoft Graph PowerShell

First, connect to Graph PowerShell:

PowerShell

```
Connect-MgGraph -Scopes "User.ReadWrite.All"
```

This example sets the password for the account ConferenceRoom01@contoso.com to never expire.

PowerShell

```
Update-MgUser -UserId ConferenceRoom01@contoso.com -PasswordPolicies
DisablePasswordExpiration -PassThru
```

Assign a meeting room license

After you create the resource account, you need to assign a license to it. The resource account needs a Microsoft Teams Rooms Basic or Teams Rooms Pro license to sign into a Microsoft Teams Rooms device. For more information, see Microsoft Teams Rooms licenses.

> **Note**
>
> Microsoft Teams Rooms Basic and Microsoft Teams Rooms Pro are the two available SKUs for shared meeting room devices, including Teams Rooms. A Teams Shared Device license is required for Teams displays with hot-desking.

To assign licenses using the Microsoft 365 admin center, do the following:

1. Sign in to the Microsoft 365 admin center.
2. Provide the admin credentials for your Microsoft 365 tenant.
3. Go to **Users** > **Active users**.
4. Select the resource account you created earlier.
5. In the right pane, select **Licenses and Apps**.
6. Expand the **Licenses** section, select the license you purchased earlier.

Next steps

Meeting policies

You may need to apply custom network, bandwidth, or meeting policies to this account. For more information on network and bandwidth policies, see Meeting policy settings for audio & video. For Teams Rooms, we recommend you set the meeting policy bandwidth to 10 Mbps.

For collaboration purposes, turn on PowerPoint Live, Whiteboard, and shared notes. It is recommended that you enable the meeting policy setting "Meet now in private meetings". You may want to create a meeting policy to adjust participants and guest settings for Teams Rooms. For example, review the lobby settings such as which attendees to automatically admit to meetings. For more information on Teams meeting policies, see Manage meeting policies in Microsoft Teams.

Calling

There are no unique requirements to enable calling with resource accounts. You enable the resource account for calling in the same way you enable a regular user.

> ⓘ **Note**
>
> We recommend turning off voice mail for shared devices by assigning a calling policy to the device resource accounts. See **Calling and call-forwarding in Teams** for more information.

To help your users more easily schedule meetings in a Teams Room, you can create room lists and places in Exchange Online.

Exchange room lists and Outlook Places are used to control which resource accounts (and therefore the Teams Rooms they're associated with) appear in Outlook's Room Finder. Room Finder is an Outlook feature that helps users find rooms that are near them, available for reservation, and meet other criteria such as the availability of a display.

Room lists are a special type of Exchange distribution group that let you group resource accounts (and therefore the Teams Rooms they're associated with) together in a meaningful way. For example, you might want to create room lists for all the rooms in each building on your campus.

Outlook Places lets you set specific attributes about a resource account and its Teams Room. Some of the attributes you can set are:

- Building
- City

- Capacity
- Whether the location is wheelchair-accessible
- Audio, video, and display names

Using a combination of room lists and place attributes selected by a user, Room Finder in Outlook will show a list of rooms available to them for reservation. To make the best use of room lists and places, create room lists based on a place attribute, such as building. For example, set the city and building place attributes for each resource account, and then add each resource account to a building room list. When a user tries to choose a room to reserve, Outlook will show a list of cities and the room lists available in each of those cities.

> **Important**
>
> Each resource account needs to have its place attributes set. If these attributes, especially city, building, and capacity, aren't set, those rooms won't show up as available options for reservation even if a room list contains them.

To create a room list, follow the instructions in Create a rooms list.

To configure the place attributes for a resource account, see Set-Place.

Related articles

Configure accounts for Microsoft Teams Rooms

Plan for Microsoft Teams Rooms

Deploy Microsoft Teams Rooms

Manage Microsoft Teams Rooms

Microsoft Teams Rooms Licensing

Migrate to Windows 10/11 Pro or Enterprise on Surface Hub 2

Article • 01/18/2023 • Applies to: Surface Hub 2S, Windows 10, Windows 11

- Article version history

Surface Hub 2S comes with Windows 10 Team installed. This customized edition of Windows 10 facilitates collaboration in meeting-room environments. You can now instead run Windows 10/11 Pro or Enterprise to use your Surface Hub 2S much like any other PC.

> **Important**
>
> This migration process requires you to follow the specific procedure that's described in this article. Before you continue, read **Solution components** and **Migration and installation workflow**.

> **Note**
>
> When you install Windows 10/11 Pro or Enterprise on your Surface Hub 2S, you need a new license that's distinct from the existing Windows 10 Team license provided with the device.

Start the migration from Windows 10 Team by using a separate PC and the downloadable *Surface UEFI Configurator* tool. The tool creates a package that contains a new UEFI setting that you apply to the Surface Hub 2S.

Surface UEFI Configurator works as an interface into Surface Enterprise Management Mode (SEMM). It enables centralized management of firmware settings on Surface devices in a corporate environment. For more information, see Microsoft Surface Enterprise Management Mode.

Solution components

- Surface Hub 2S device running Windows 10 Team
- Separate device running Windows 10
- Surface UEFI Configurator tool to create the SEMM package
- Windows 10/11 Pro or Enterprise OS image, version 20H2 or later

- Two USB drives that have 16 GB of storage, FAT32 format
- The drivers and firmware for Windows 10 Pro and Enterprise in a Surface Hub 2 Microsoft Windows Installer (MSI) file
- Internet connection
- Imaging solution (optional)

Migration and installation workflow summary

Step	Action	Summary
1	Verify the UEFI version on the Surface Hub 2S.	The UEFI version must be version *694.2938.768.0* or later.
2	Download Surface UEFI Configurator and the Surface Hub 2 drivers and firmware.	On the **Surface Tools for IT** page, select **Download**. Then select and download the **Surface UEFI Configurator MSI file**, and install it on a separate PC. Also download the Drivers and firmware for Windows 10 Pro and Enterprise OS on Surface Hub 2 MSI file. Save this package for use in step 5.
3	Prepare the SEMM certificate.	Prepare the certificate that's required to run Surface UEFI Configurator, or use your current certificate.
4	Create a SEMM package.	Start Surface UEFI Configurator to create a SEMM package on a USB drive. This package will contain the configuration files you need to apply on Surface Hub 2S. Copy these SEMM package files to a folder on your PC.
5	Load a USB flash drive with Windows 10 image, the SEMM package, and drivers and firmware.	Create a USB drive that contains a Windows 10 image. In this example, the drive is named *BOOTME*. Add the drivers and firmware for Windows 10 Pro and Enterprise OS on Surface Hub 2 (from step 2) and the SEMM package files (from step 4) to the *BOOTME* drive.
6	Update the UEFI on the Surface Hub 2S to enable OS migration.	Use the *BOOTME* drive to boot the Surface Hub 2S to the UEFI menu and install the SEMM package.
7	Install Windows 10 Pro or Enterprise.	Use the *BOOTME* drive to install Windows 10 Pro or Enterprise version *20H2* or later.
8	Install drivers and firmware for Windows 10 Pro and Enterprise.	To ensure that your device has all the latest updates and drivers, install the Drivers and firmware for Windows 10 Pro and Enterprise OS on Surface Hub 2 MSI file.

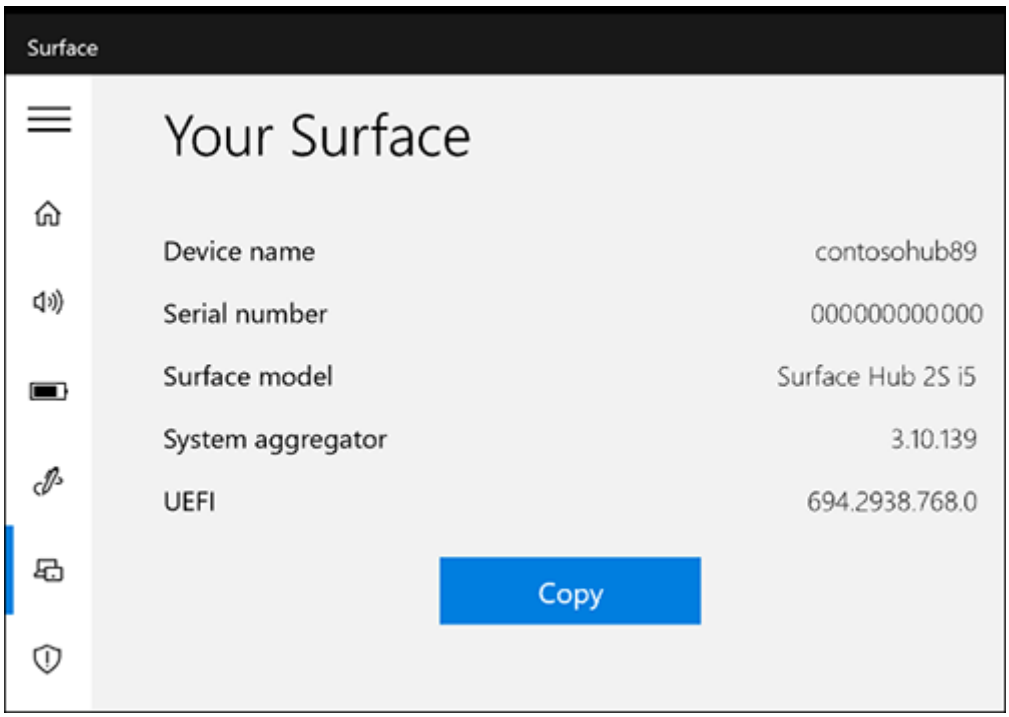
Step	Action	Summary
9	Configure Surface Hub 2S as a personal productivity device.	Enable the recommended settings and applications to optimize Surface Hub 2S as a personal productivity device.

Verify the UEFI version on Surface Hub 2S

Before you migrate Surface Hub from Windows 10 Team to Windows 10 Desktop, you need UEFI version *694.2938.768.0* or later.

To verify the UEFI version on your system:

1. On the Surface Hub 2S home page, select **Start**, and then open the Surface app (**All Apps** > **Surface**).
2. Select **Your Surface** to display information about Surface Hub, including the current UEFI version on the device.
    - If the UEFI version is *694.2938.768.0* or later, as the following image shows, you can create the SEMM package to enable OS migration.



    - If the UEFI version is earlier than version *694.2938.768.0*, use one of the following methods to get a newer version

Update UEFI via Windows Update

1. On your Surface Hub 2S, sign in as **Admin**.

   > **Note**
   >
   > If you don't know your user name or admin password, you'll need to reset the device. For more information, see **Reset and recovery for Surface Hub 2S**.

2. Go to **All apps** > **Settings** > **Update and Security** > **Windows Update**, and install all updates.

3. Restart the device.

4. Verify the UEFI version by using the Surface app. If the UEFI version isn't version *694.2938.768.0* or later, repeat these steps, or use the following procedure to get the latest UEFI version.

Update the UEFI via bare metal recovery (BMR) image

1. Go to the Surface recovery site and select **Surface Hub 2S**.

2. Enter your Hub serial number. It's located on the back of the Hub next to the power connection.

3. Follow the directions to download the image onto a formatted USB drive by installing the Windows 10 Team 2020 Update.

4. After the update, the device enters out-of-box-experience (OOBE) setup. You don't need to complete setup. The UEFI version is already updated. Instead power down the device by holding the power button until the screen turns off.

Download Surface UEFI Configurator and Surface Hub 2 drivers and firmware

On a separate PC, follow these steps:

1. On the Surface Tools for IT page, select **Download**.

2. Select and download the Surface UEFI Configurator MSI file, and install it on a separate PC. The Surface UEFI Configurator tool can't be run on a Surface Hub 2S while Windows 10 Team edition is installed.

3. Download the Surface Hub 2 drivers and firmware Windows Installer MSI file. You'll use this file when you install the new operating system.

Prepare the SEMM certificate

If you haven't used Surface UEFI Configurator before, you need to prepare a certificate. This certificate ensures that after a device is enrolled in SEMM, you can modify UEFI settings only by using packages that are created with the approved certificate.

How you get a certificate depends on the size or complexity of your organization:

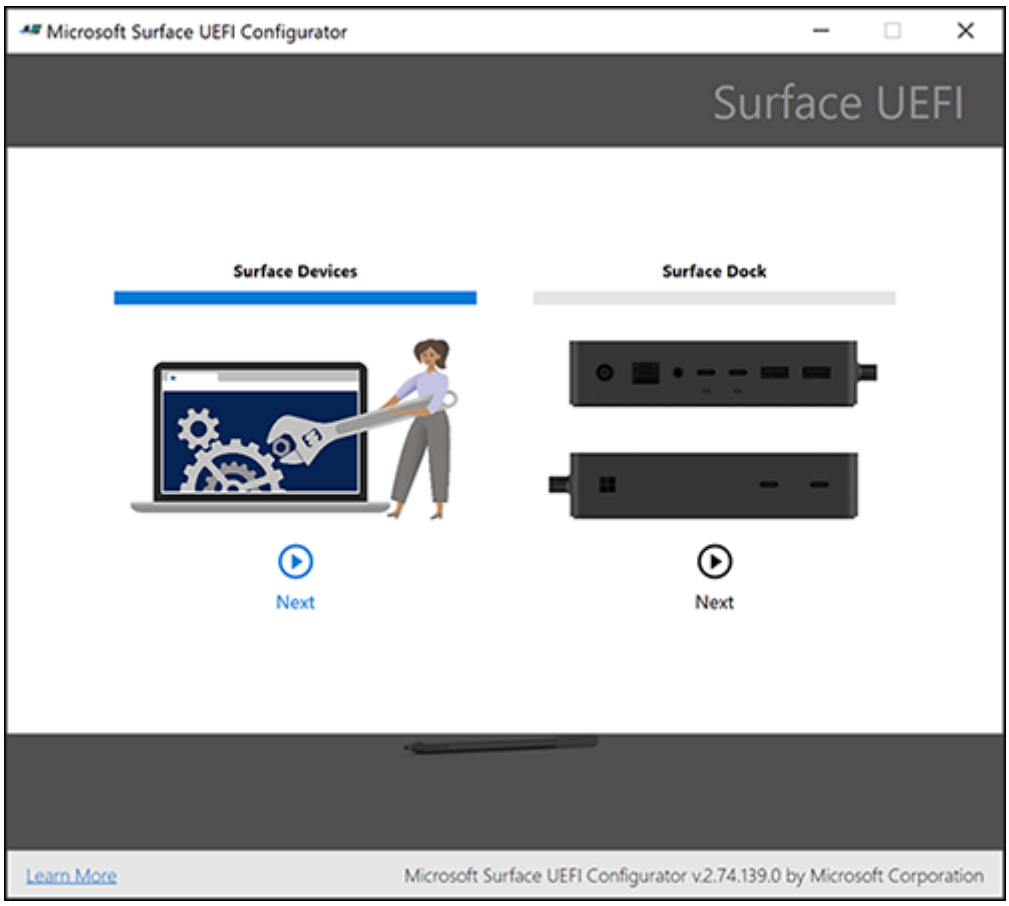
- Enterprise organizations typically maintain their own infrastructure to generate certificates according to standard security practices.
- Medium-sized businesses and others often choose to get certificates from partner providers. This option is recommended for organizations that don't have as much IT expertise or lack a dedicated IT security team.
- Alternatively, you can generate a self-signed certificate by using a PowerShell script. For more information, see the Surface Enterprise Management Mode certificate requirements. Or you can use PowerShell to create your own certificate. For more information, see the Self-signed certificate documentation.

The SEMM package that Surface UEFI Configurator creates must be secured with a certificate. The certificate verifies the signature of configuration files before UEFI settings can be applied. For more information, see the SEMM documentation.

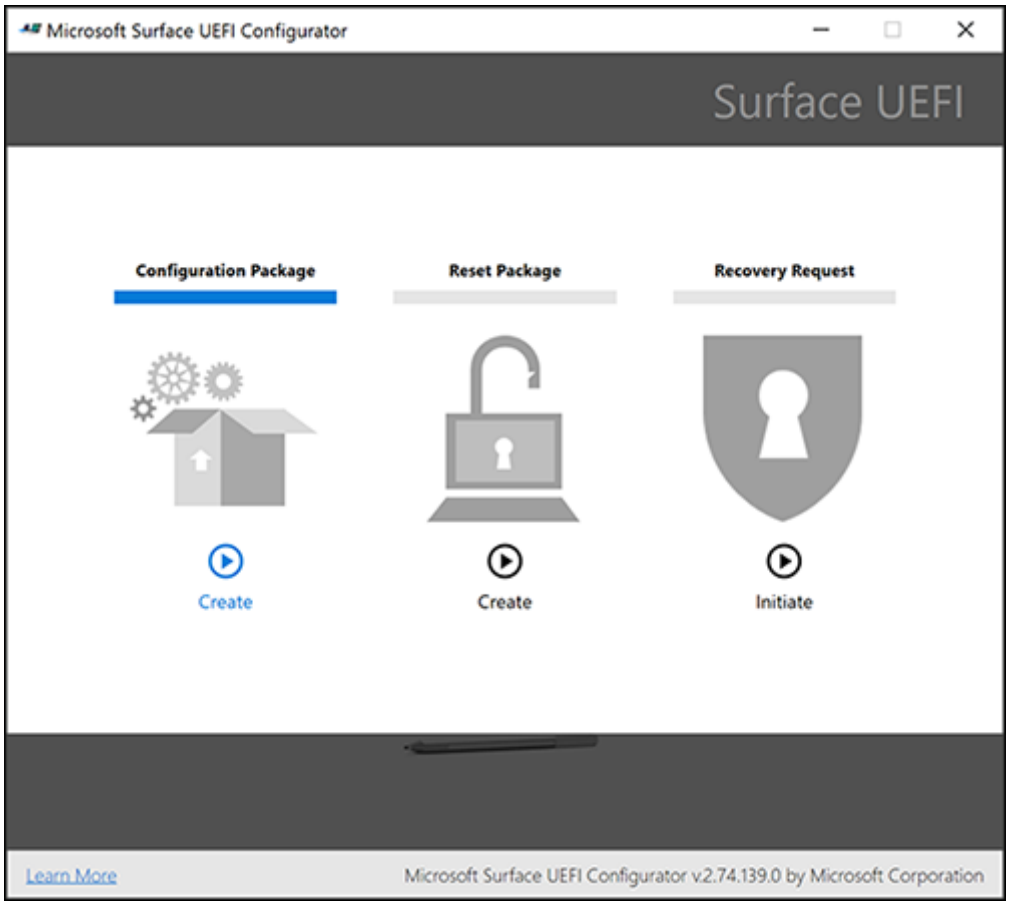
Create a SEMM package

1. On a separate PC, install the Surface UEFI Configurator tool that you downloaded earlier.
2. Open Surface UEFI Configurator, and then select **Start**.

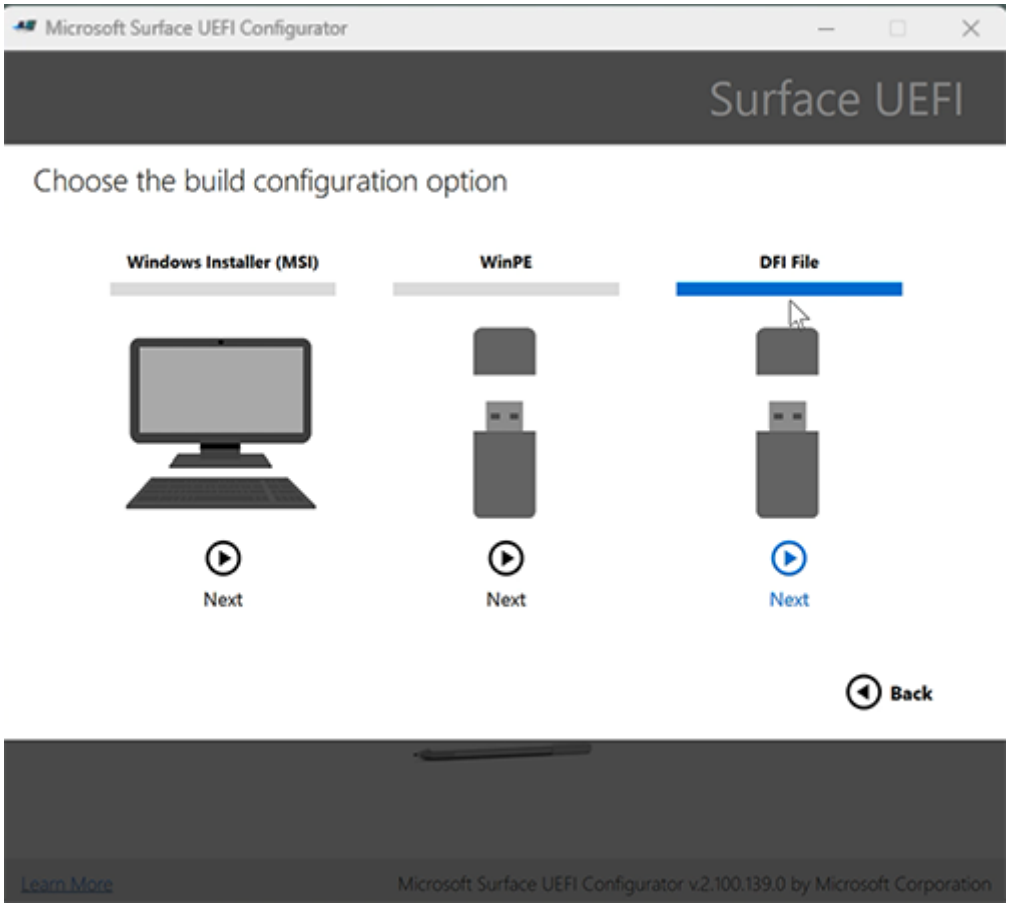
3. Select **Surface Devices**, and then select **Next**.



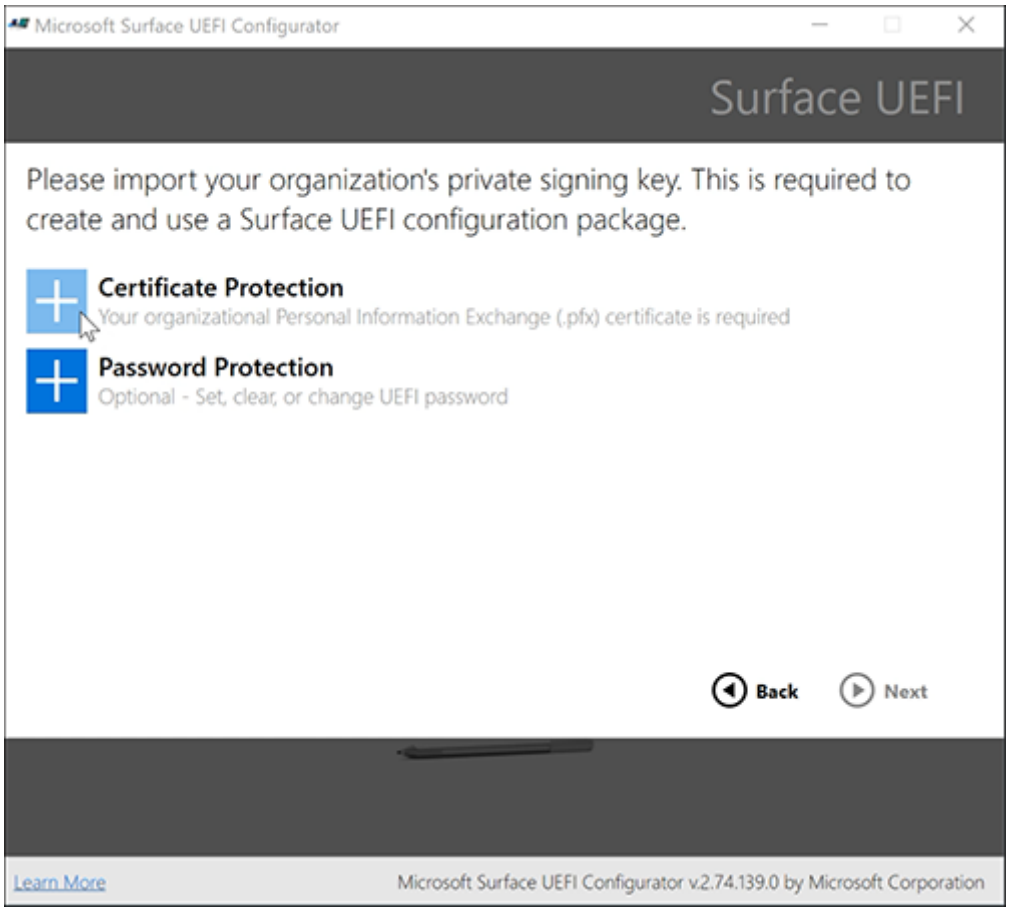
4. Select **Configuration Package**.



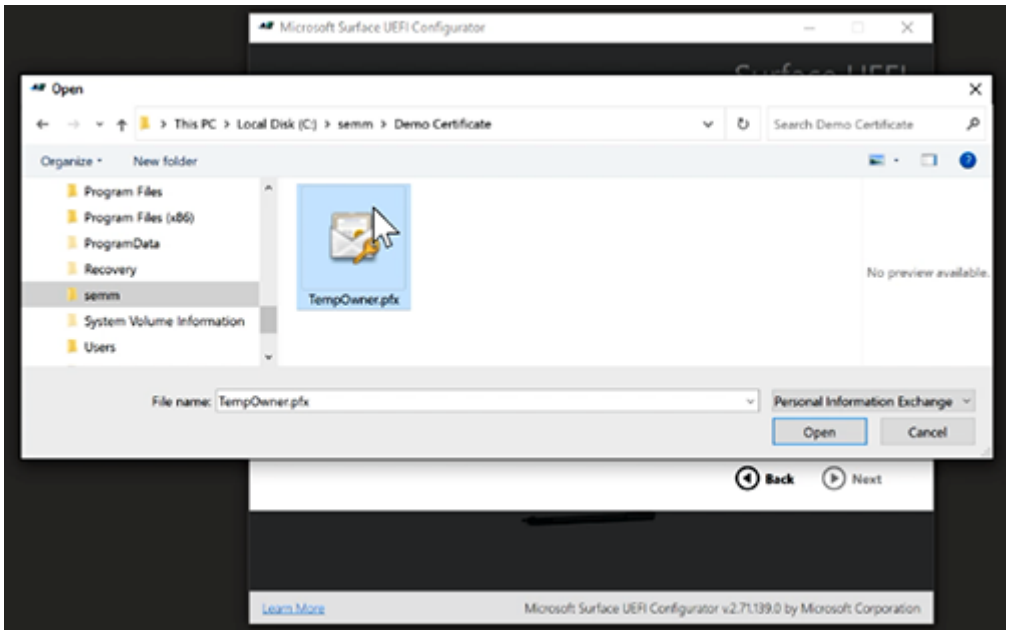
5. Select **DFI File**.



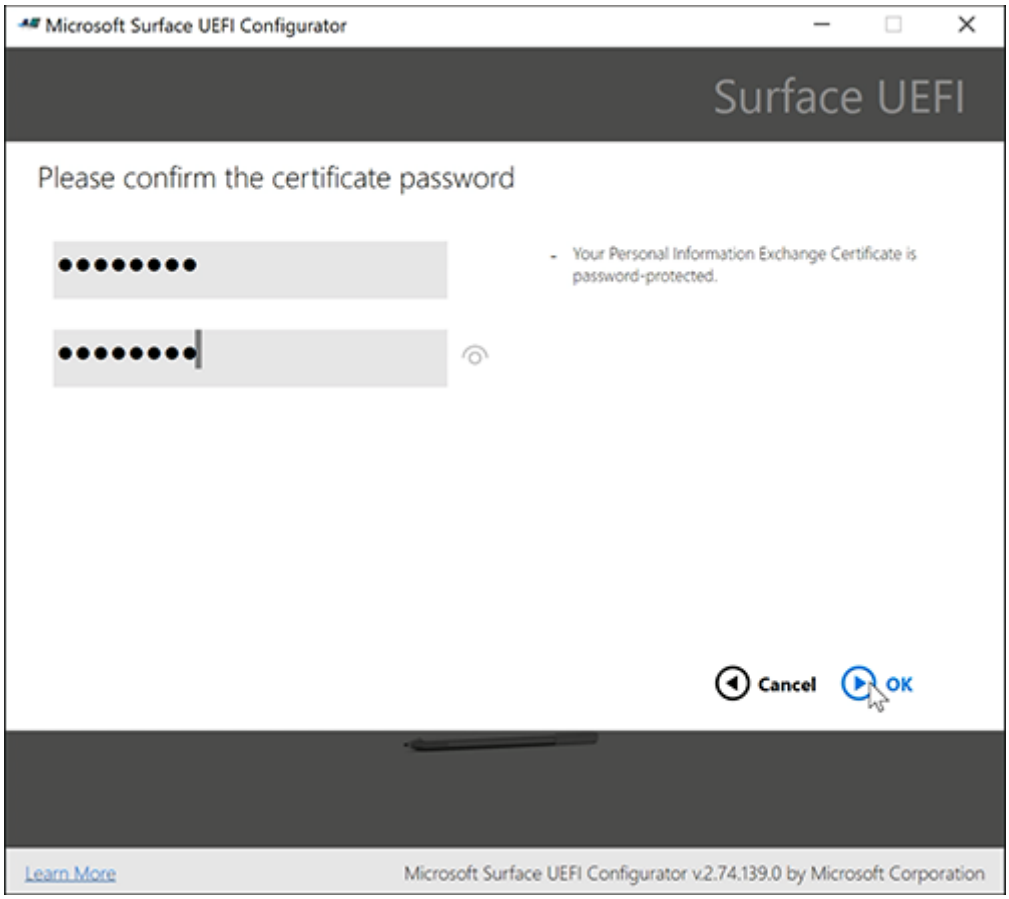
6. Select **Certificate Protection**.



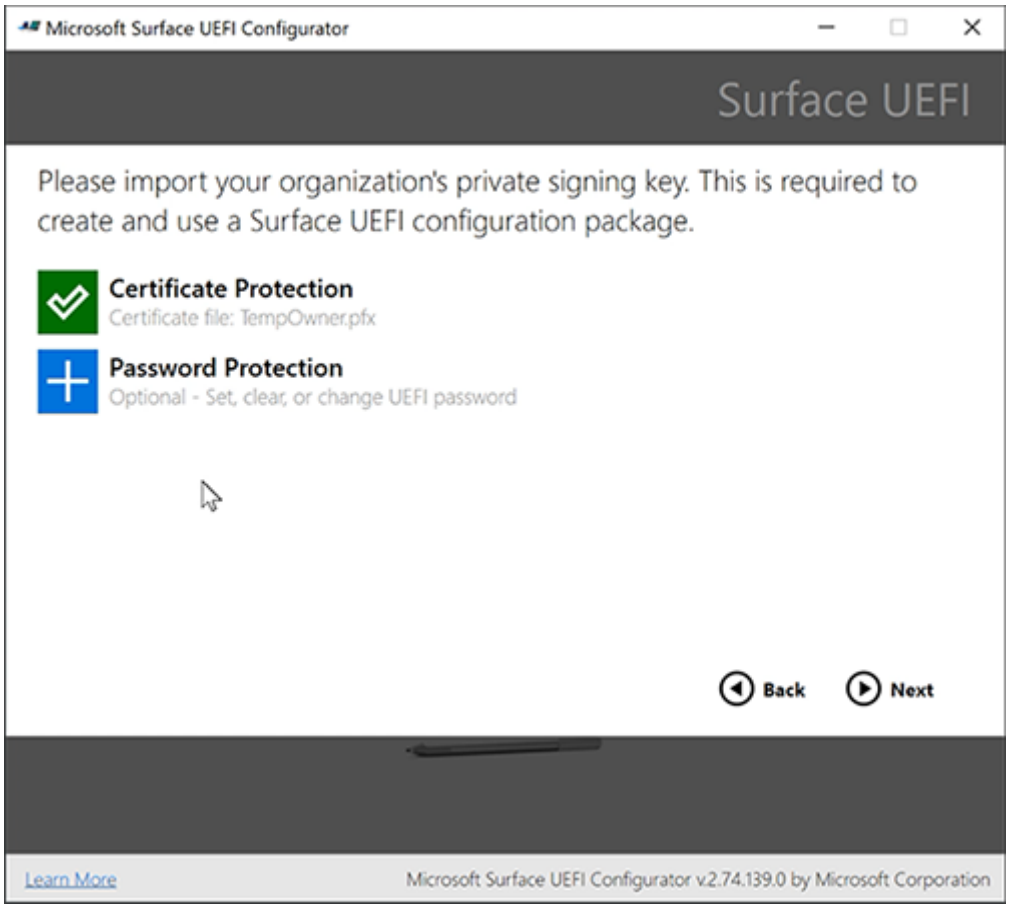
You'll be prompted to add your certificate .pfx file.



7. Enter your certificate password, and then select **OK**.

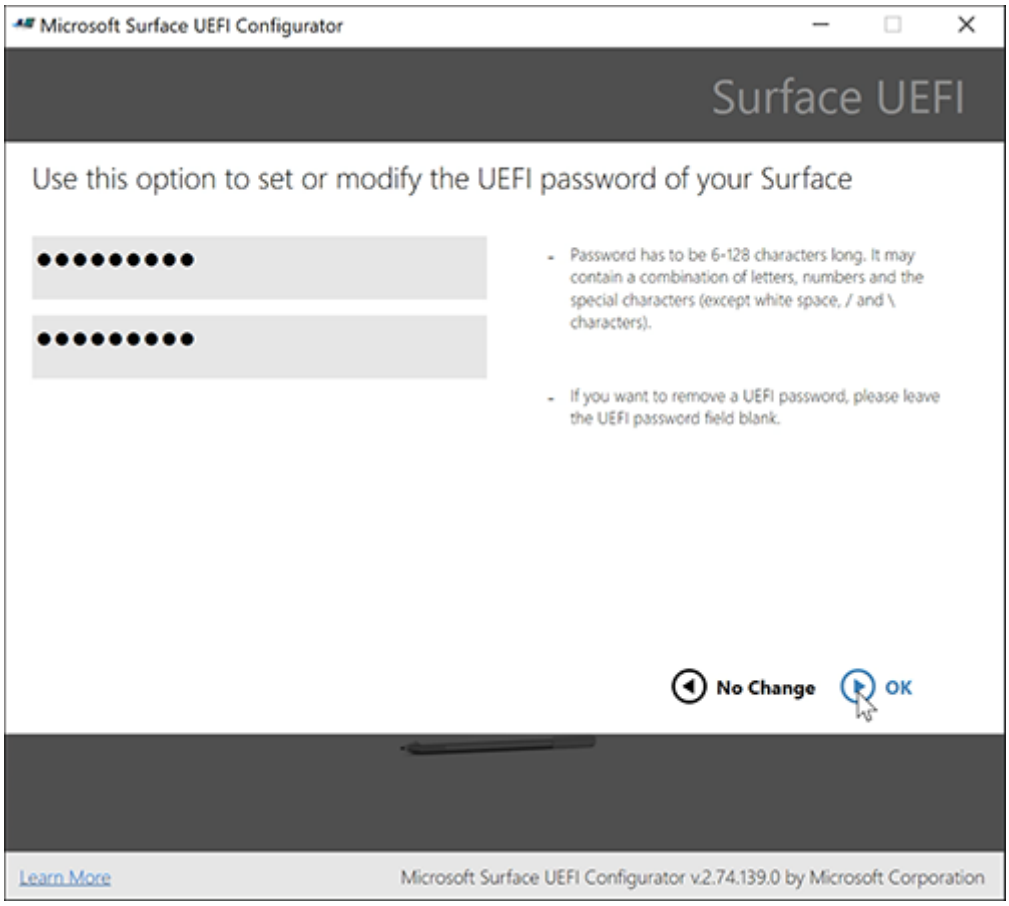


8. Select **Password Protection** to add a password to the Surface UEFI. You'll need this password whenever you boot to the UEFI. *We strongly recommend that you set a UEFI password that you'll use on Surface Hub 2S.*

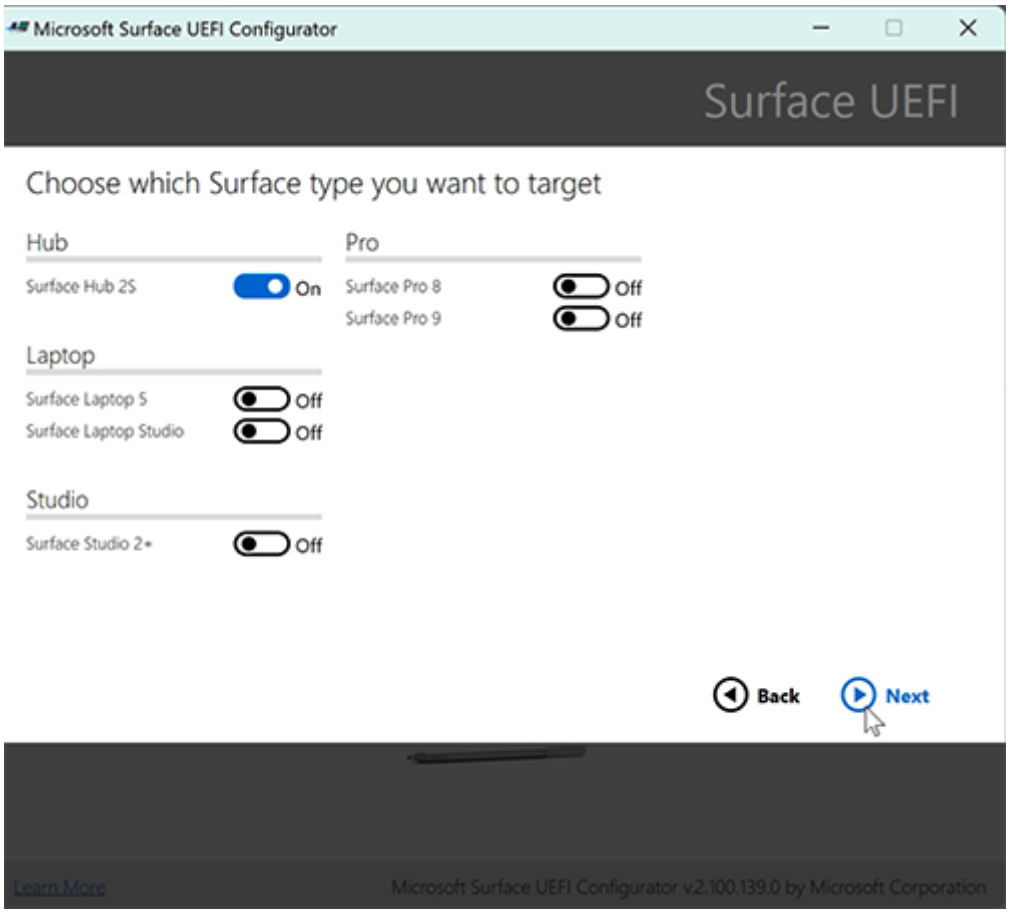


9. Set a UEFI password, and then select **OK**.

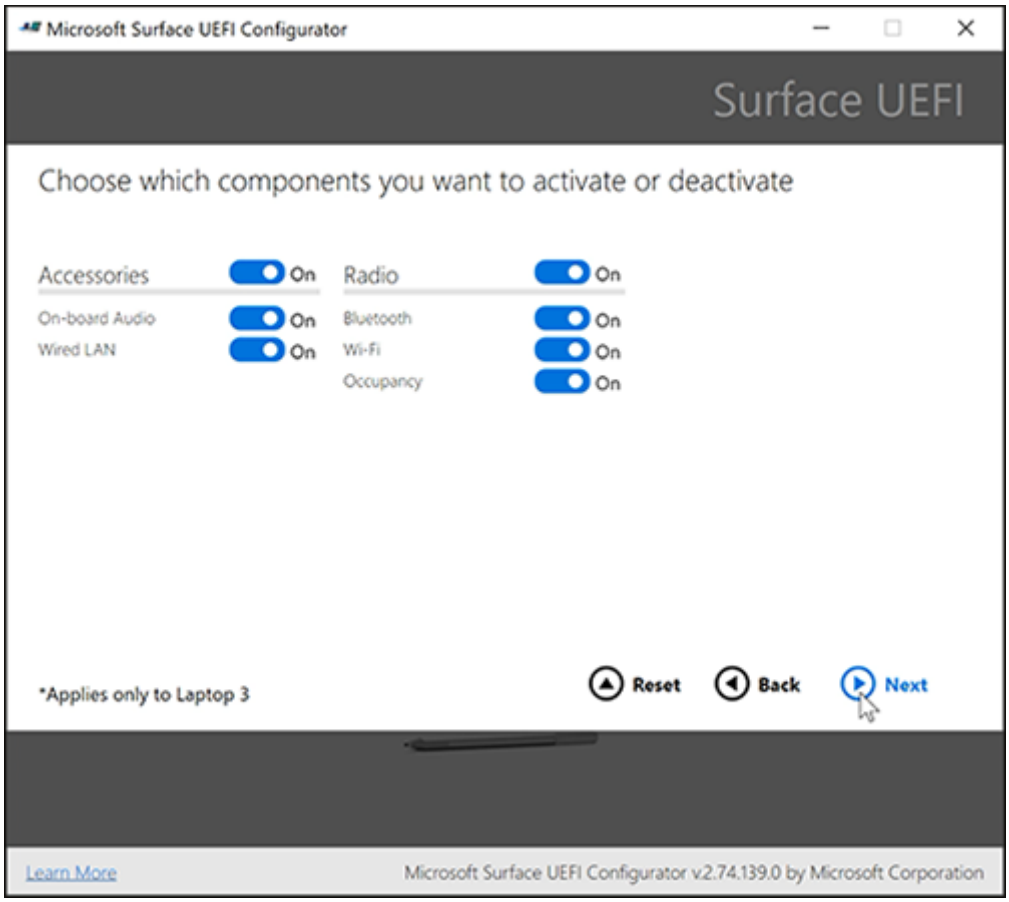
> **ⓘ Important**
>
> Save the password in a secure location that's accessible to your IT admins who manage Surface Hub. *If this password is lost, it can't be recovered.*



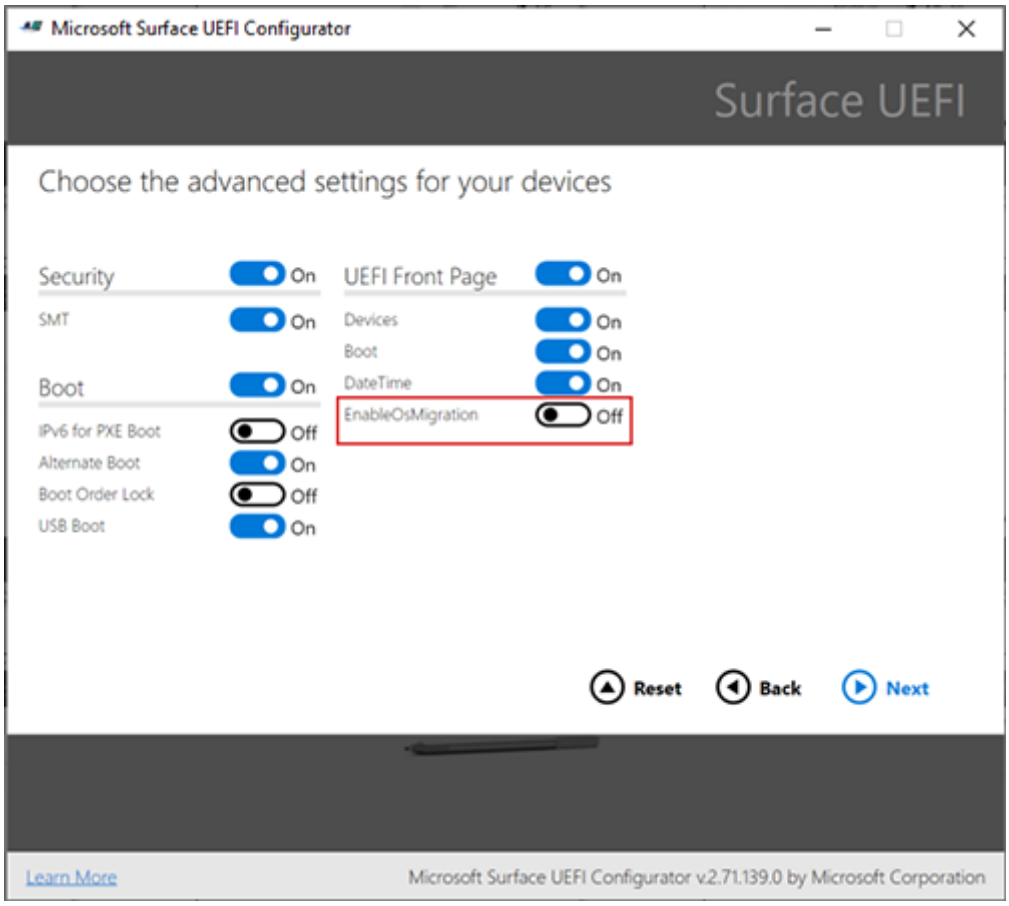
10. Select **Surface Hub 2S**, and then select **Next**.

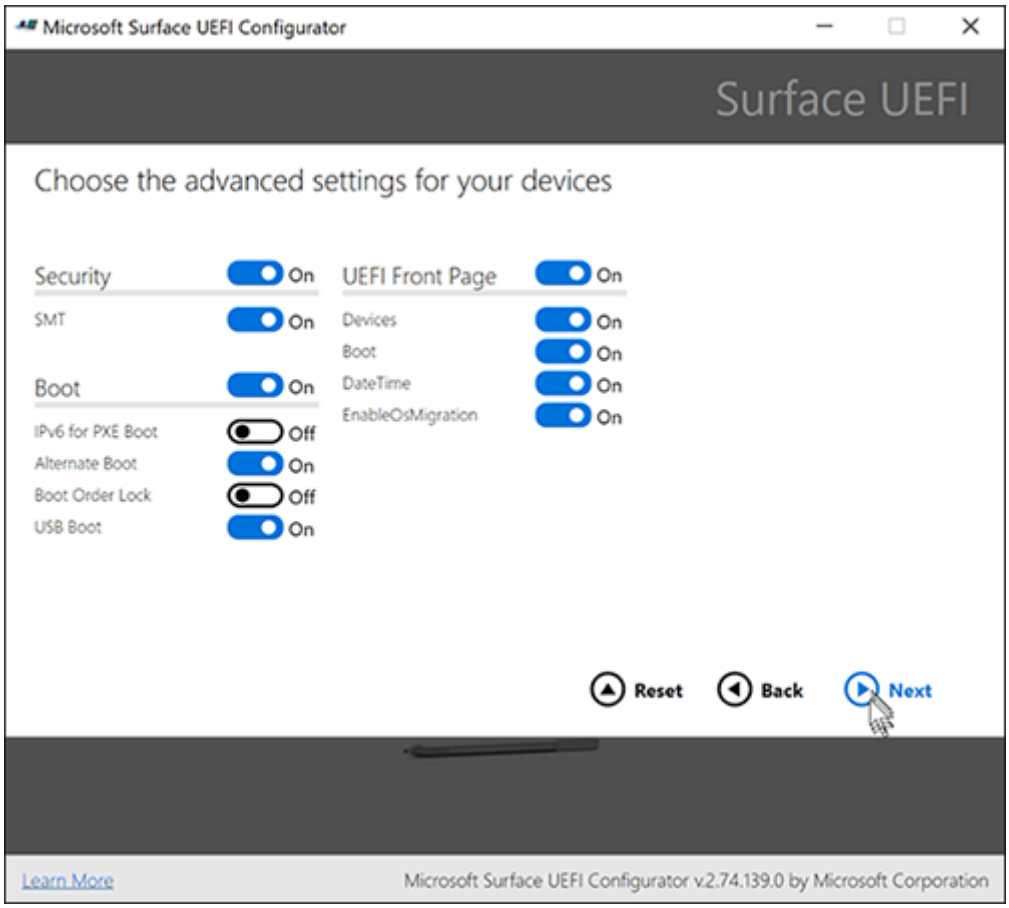


11. Select **Next** again.



12. To allow installation of Windows 10/11 Pro or Enterprise, turn on **EnableOsMigration**, and then select **Next**.





Manage SEMM enrollment

Enrolling a device into SEMM affects how you can manage it. For example, after you apply a SEMM package, all UEFI settings are unavailable (locked) in the device's UEFI menu. Default values for other settings such as **IPv6 for PXE Boot** are also unavailable.

To change UEFI settings after you finish the migration, apply another SEMM package or unenroll the device from SEMM. If you apply another SEMM package to change the UEFI settings, you must use the original certificate when you build the new SEMM package. Use the UEFI Configurator tool and leave **EnableOSMigration** *off* (not *on* as in the original migration steps).

If you work with partners

If your company outsources the Surface Hub 2 migration to Windows 10/11 Pro or Enterprise, you may want to have the partner transfer the SEMM certificate, SEMM package, and UEFI password to you. Or, after you migrate the Hub, you can immediately unenroll it from SEMM. This step enables local administration of UEFI and transfer of the device to another party. But we still strongly recommend that you use a UEFI password, which can be configured after migration. To learn more, see Manage Surface UEFI settings.

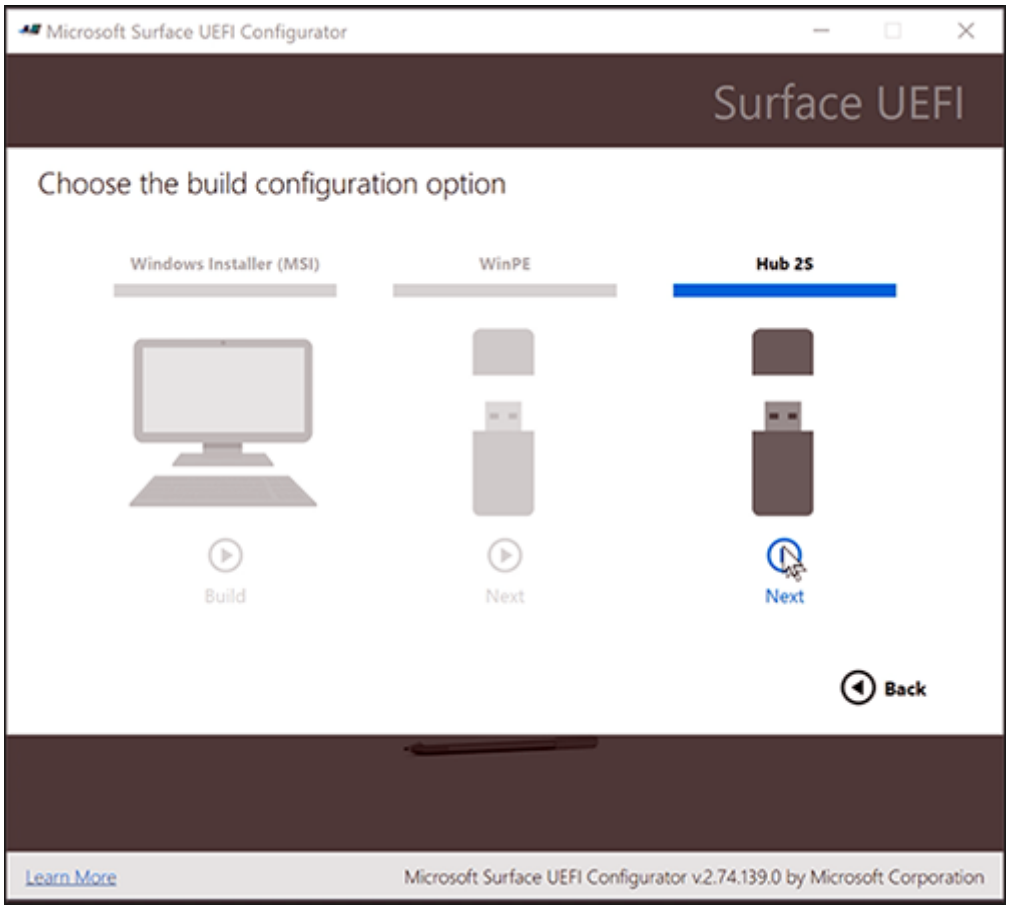
To roll back to Windows 10 Team

If you choose to restore your device to Windows 10 Team after the migration as described later in this article, we recommend that you first unenroll Hub from SEMM. To learn more, see Unenroll Surface devices from SEMM.

> ⚠ **Warning**
>
> To unenroll a device from SEMM and restore user control of Surface UEFI settings, you must have the SEMM certificate that was used to enroll the device in SEMM. If this certificate becomes lost or corrupted, it is not possible to unenroll from SEMM. Back up and protect your SEMM certificate accordingly.

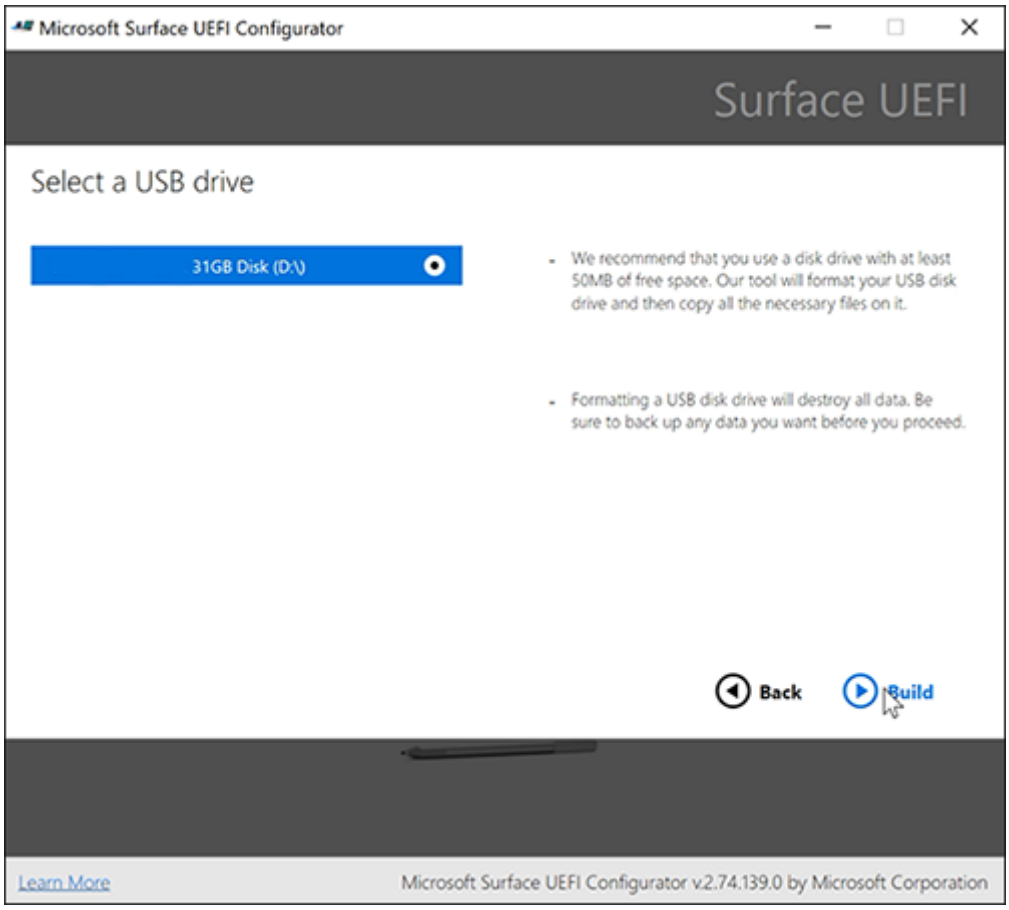
Save the SEMM package to a USB drive

1. Connect a USB drive to your PC.
2. Choose **Hub 2S**, and then select **Next**.

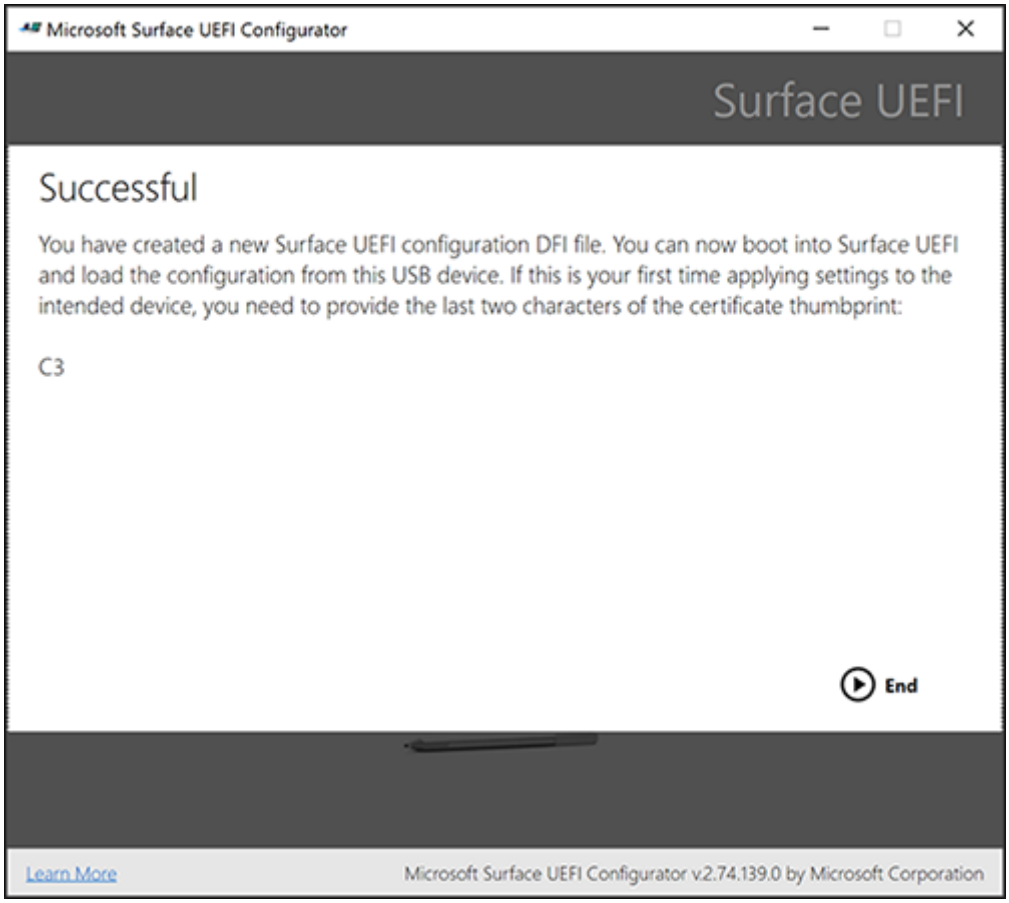


> ⚠ **Warning**
>
> All existing data on the USB drive will be erased when the SEMM package is built. Before you build the SEMM package, remove any files that you need from the USB drive.

3. Select **Build**.



4. Capture a screenshot of this page, and then select **End**. Your SEMM package is now ready. It contains the SEMM package *DfciUpdate.dfi* and a text file that includes the SEMM *thumbprint*, which is the last two characters of the certificate's thumbprint.



5. Save the certificate thumbprint's last two characters. You'll need these characters to activate SEMM when you apply the package on Surface Hub 2S.

Load a USB flash drive with a Windows 10 image, SEMM package, and Surface Hub 2 drivers and firmware

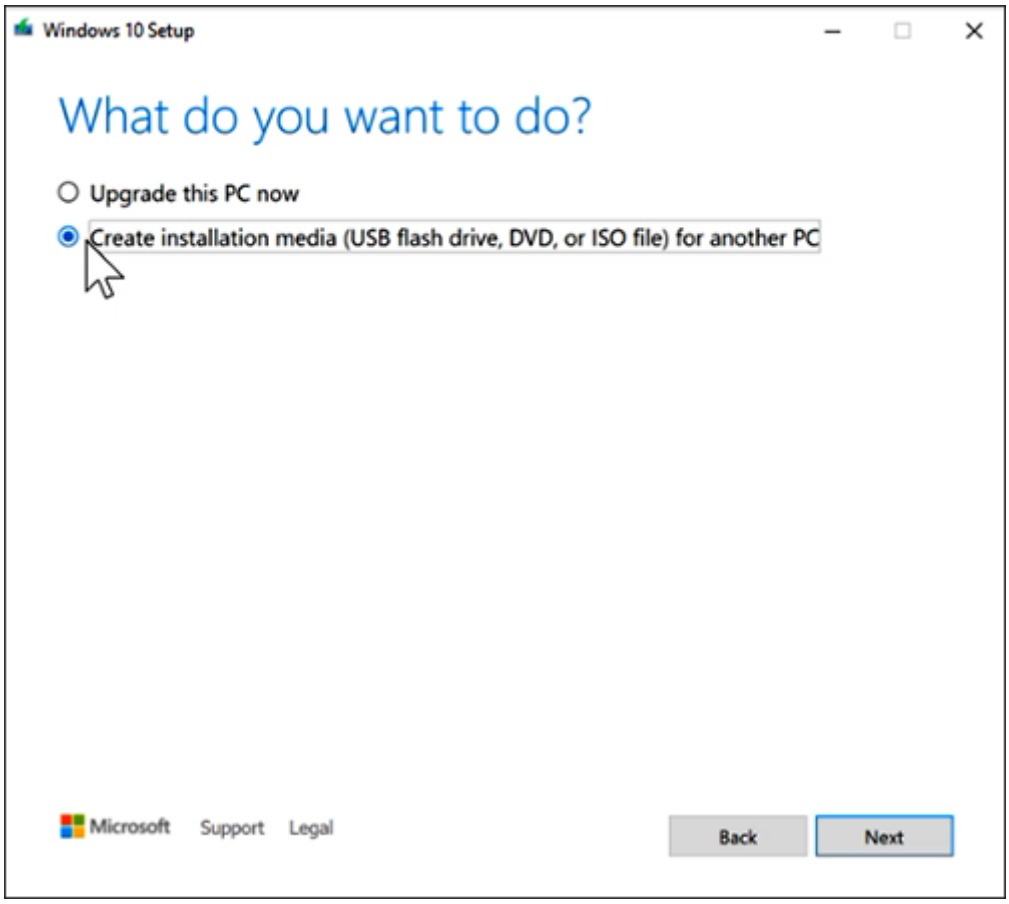
You can install a Windows 10/11 Pro or Enterprise image (version *20H2* or later) by using one of the following options:

- Your current imaging solution.
- Surface Deployment Accelerator. Use this tool to create a bootable Windows 10 image. The image can include all current Windows 10 updates, Microsoft Office, other apps, and the required drivers and firmware.
- A USB flash drive that contains a Windows 10/11 Pro or Enterprise image. This option will not have Wi-Fi available until after out-of-box-experience (OOBE) setup. Once setup is complete, install the required Surface Hub 2 drivers and firmware for Windows 10 Pro and Enterprise on the device.

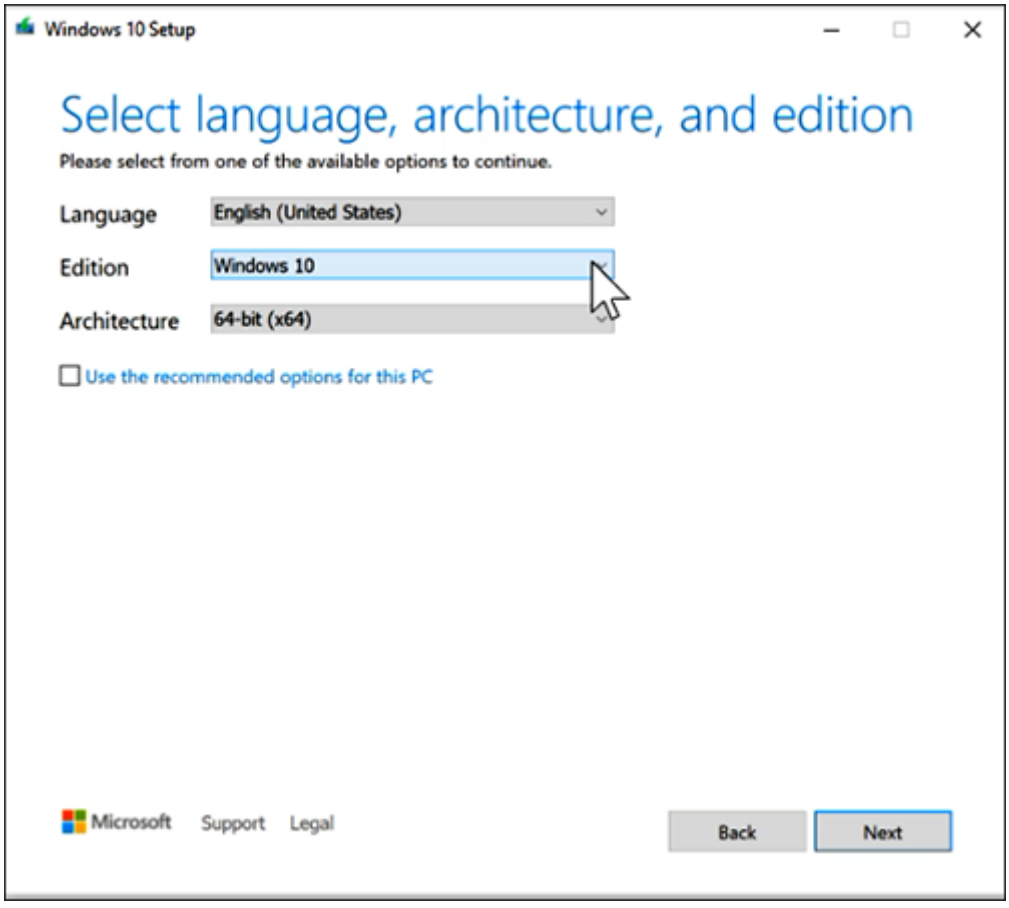
The following steps show how to create a USB flash drive from installation media and then add the SEMM package files and the drivers and firmware for Windows 10 Pro and Enterprise OS on Surface Hub 2 MSI file. If you use another deployment method, go to the Update UEFI on Surface Hub 2S to enable OS migration section of this article.

> **Note**
>
> After you finish the installation, you'll need a valid license for Windows 10 Pro or Windows 10 Enterprise that's separate from your existing Windows 10 Team license.

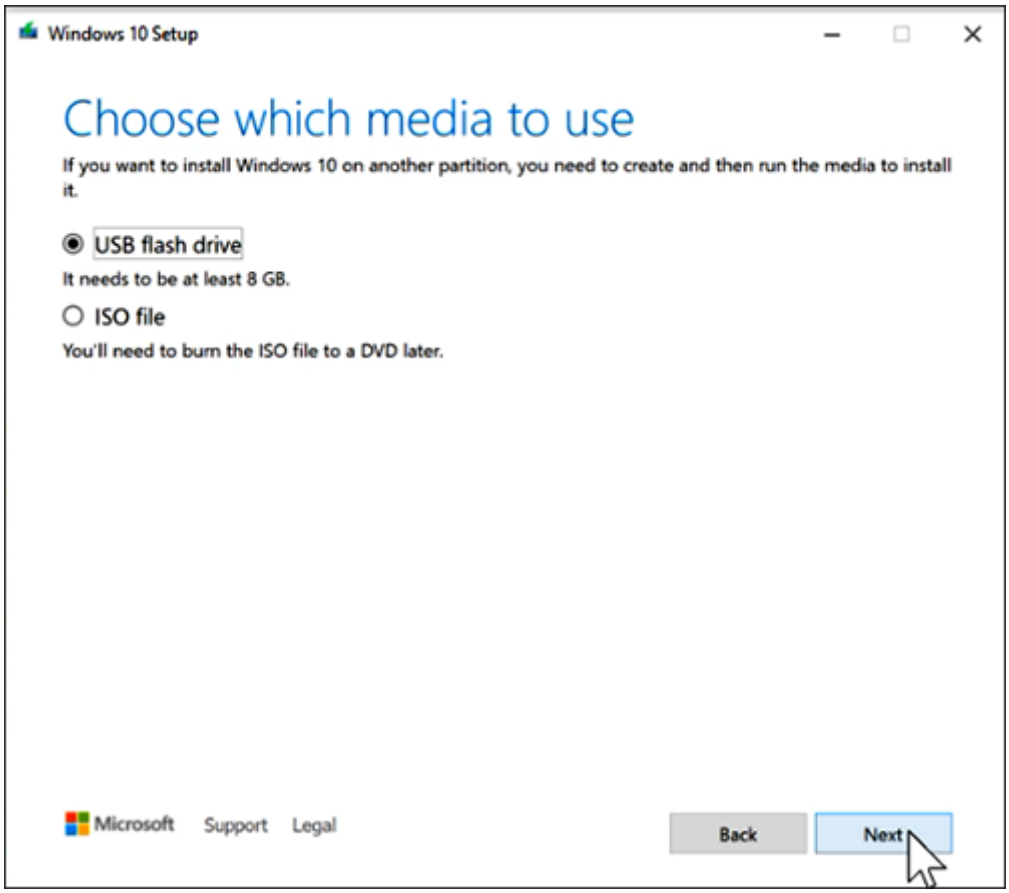
1. To create a Windows 10 Pro installation, follow the instructions to download the media creation tool at Download Windows 10. To download Windows 10 Enterprise, go to the Microsoft Volume Licensing Service Center.
2. Insert a new USB storage drive.
3. Open the media creation tool, select **Create installation media**, and then select **Next**.



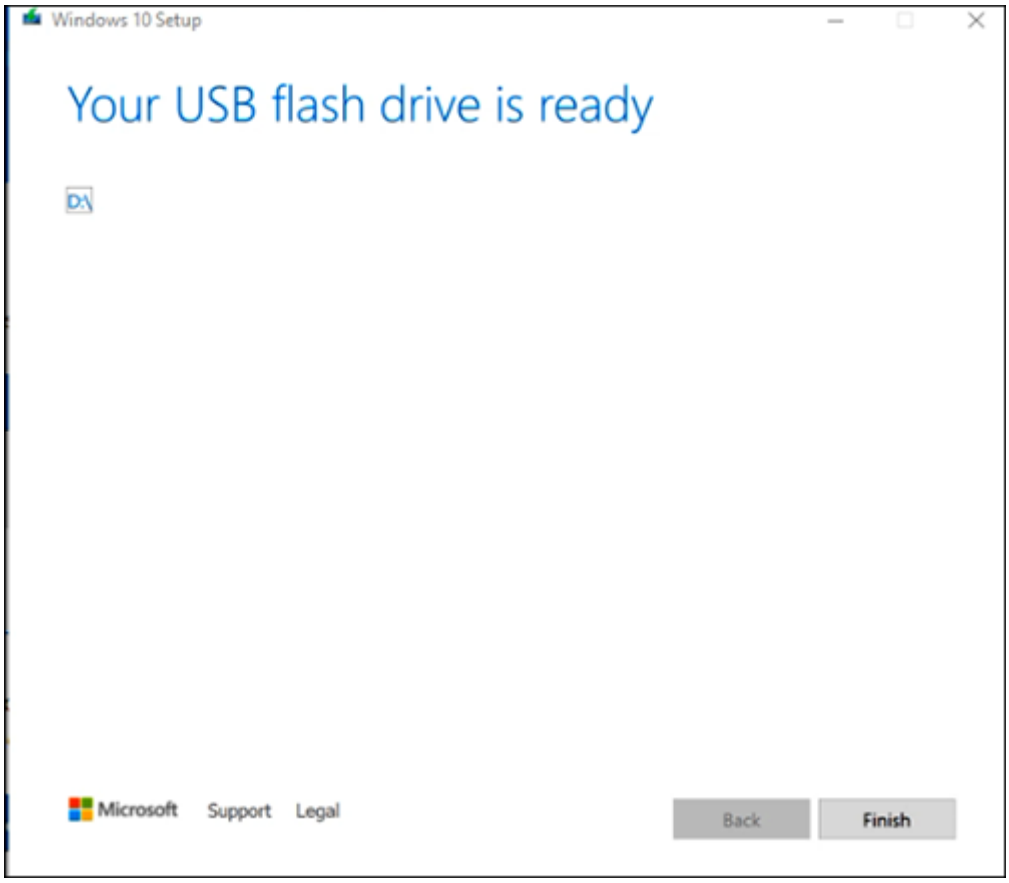
4. Select a language, and then select **Windows 10** and **64-bit (x64)**. Then select **Next**.



5. Select **USB flash drive**, and then select **Next**.



6. When the download finishes, select **Finish**.



7. Copy the SEMM package files and the drivers and firmware for Windows 10 Pro and Enterprise OS on Surface Hub 2 (the MSI file) to the root of the USB flash drive

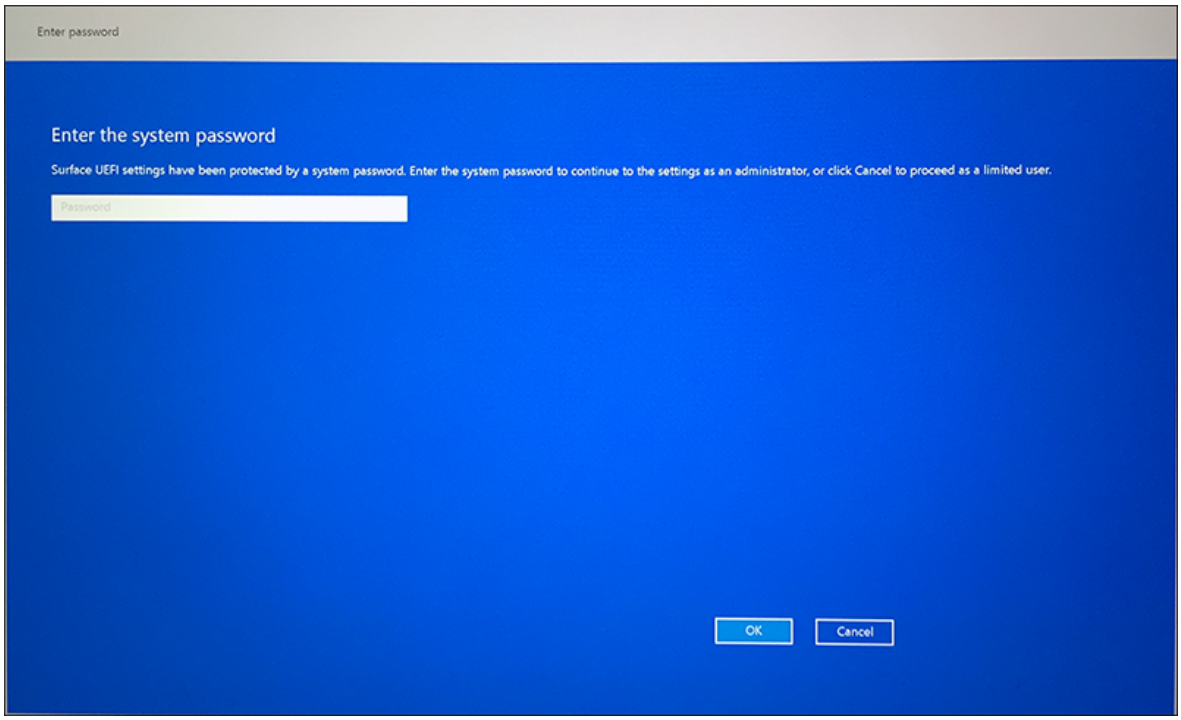
(*BOOTME*) that contains your Windows 10 image. The BOOTME USB drive will contain:

- Your Windows 10 bootable image.
- The SEMM package files, copied to the root of the USB drive:
  - *DfciUpdate.dfi*.
  - A text file that includes the SEMM thumbprint. (In this example, the file is *SurfaceUEFI_2020Aug25_1058.txt*.) The automatically generated date-time stamp corresponds to the date that you created the file by using Surface UEFI Configurator.
- The drivers and firmware for Windows 10 Pro and Enterprise OS on Surface Hub 2 (SurfaceHub2S_Win10_18362_20.082.25682.0.msi). Copy this file to the root of the USB drive.

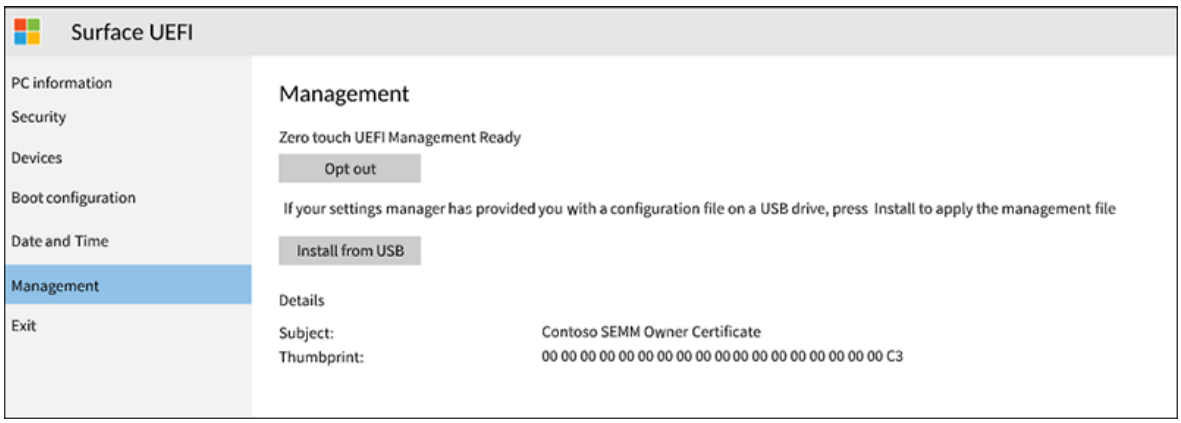
Update UEFI on Surface Hub 2S to enable OS migration

1. Insert your BOOTME drive into the USB-A port on the Surface Hub 2S. For a list of its required contents, see the previous section.
2. To boot into UEFI:
   a. Turn off (shut down) your Surface Hub 2S.
   b. Press and hold **Volume +**, and then press and release the power button. Keep holding **Volume +** until the UEFI menu appears.

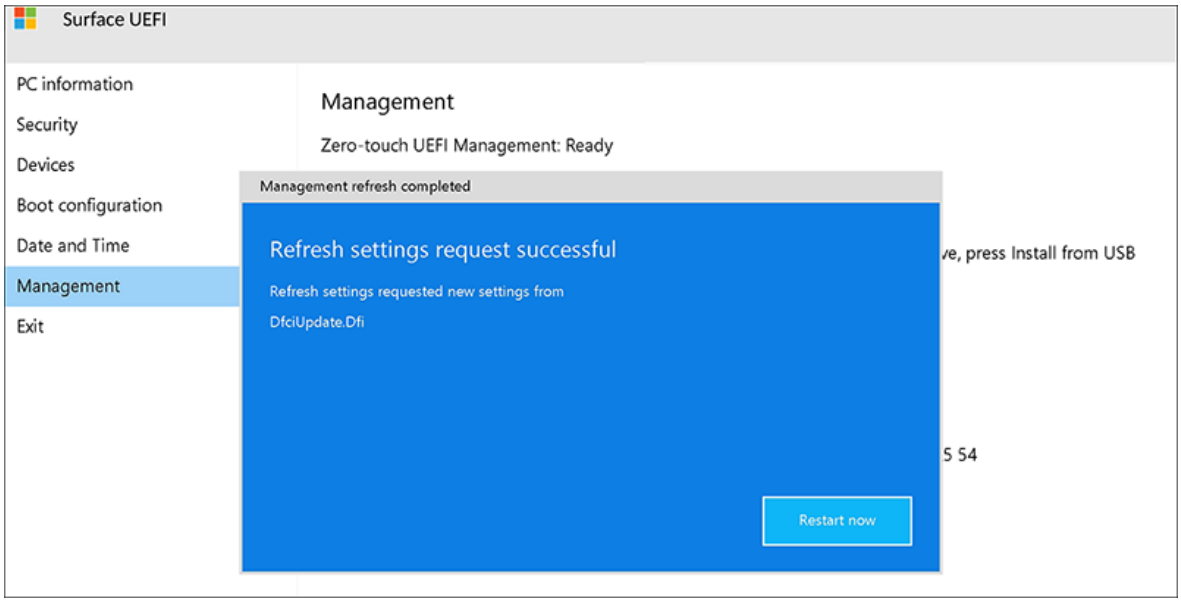
3. When the device restarts, enter the UEFI password that you created earlier, if applicable (recommended).



4. From the UEFI menu, select **Management**. Then select **Install from USB**.



5. Select **Restart now**, as the following image shows. The device will restart. It will display a white Microsoft logo in the middle of the window and then shut down.



6. Press and release the power button. In the red dialog box that appears, choose to activate Surface Enterprise Management Mode.

7. Enter your two-character certificate thumbprint and your UEFI settings password. Then select **OK**.

> ⓘ **Note**
>
> After you activate SEMM on your device, the new UEFI setting **EnableOSMigration** is applied. You can no longer access Windows 10 Team. Instead, you must continue to the next step and install Windows 10 Pro or Windows 10 Enterprise.

The device reboots. It displays the white logo in the middle of the screen and then shuts down again.

Install Windows 10/11 Pro or Enterprise

1. If your bootable Windows 10/11 Pro or Enterprise drive isn't already in the Surface Hub 2 USB-A port, insert it now. Then press and release the power button.

   When the device starts, you'll see the white logo in the middle of the screen. Then a spinning circle appears below the white logo.

2. If the Surface device doesn't automatically boot to the USB drive, power off the device (unplug the power cord and then plug it back in). After you plug in the

power cord again, the device should boot after a few seconds. Then you'll see the white logo in the middle of screen.

If the device doesn't turn on, press and release the power button. Immediately after you see the logo in the middle of the screen, press and hold the Volume down button until you see the spinning circle below the white logo.

3. When the out-of-box experience (OOBE) setup starts, follow the instructions to install Windows 10/11 Pro or Enterprise (version *20H2* or later).

Install Surface Hub 2 drivers and firmware

To ensure that your Surface Hub 2 is up to date, install drivers and firmware for Windows 10 Pro and Enterprise. Then reboot the device. Keep the Surface turned on for an hour, and then reboot it again. You won't be prompted for the second reboot. This pause and extra reboot ensures that the firmware has been fully updated.

Configure recommended settings

To configure Surface Hub 2S as a personal productivity device, see Configure Windows 10/11 Pro or Enterprise on Surface Hub 2.

> **Note**
>
> If you can't successfully migrate your device to Windows 10/11 Pro or Enterprise for Surface Hub 2 by following the steps outlined in this article, contact **Surface Hub Support**.

To roll back to Windows 10 Team

If you want to restore your device to Windows 10 Team, see Reset and recovery for Surface Hub 2S. Before you roll back to Windows 10 Team, we recommend that you first unenroll the Surface Hub from SEMM. To learn more, see Unenroll Surface devices from SEMM.

> **Warning**

To unenroll a device from SEMM and restore user control of Surface UEFI settings, you must have the SEMM certificate that was used to enroll the device in SEMM. If this certificate becomes lost or corrupted, it is not possible to unenroll from SEMM. Back up and protect your SEMM certificate accordingly.

Troubleshooting and common problems

Issue	Notes
Unable to migrate to Windows 10/11 Pro or Enterprise on Surface Hub version 1 devices	By design, the ability to migrate to Windows 10/11 Pro or Enterprise is only available for Surface Hub 2S devices.
UEFI menu does not appear when holding down the **Volume + power button**	- Ensure you are holding down both buttons for approximately 10 seconds. After you see the Windows logo, release the **power button** while continuing to hold **Volume +** - Try connecting the USB drive via **USB-C.**
The Surface Hub 2S does not automatically reboot after entering the two-character certificate thumbprint and your UEFI settings password.	Press the Surface Hub 2S **Power button** to manually power the device back up.
No audio from speakers following migration to Windows 10/11 Pro or Enterprise	To resolve, download and install the Drivers and Firmware for Windows 10 Pro and Enterprise on Surface Hub 2 (MSI).
The volume rocker button is non-functional following migration to Windows 10/11 Pro or Enterprise.	To resolve, download and install the Drivers and Firmware for Windows 10 Pro and Enterprise on Surface Hub 2 (MSI).

Issue	Notes
How do I determine the serial number of the Surface Hub 2S when running Windows 10/11 Pro or Enterprise?	You can determine the serial number of your Surface Hub 2S running Windows 10/11 Pro or Enterprise just as in the Windows 10 Team OS: *You can find the serial number on the outside of the packaging, on the display by the power cord, or by using the Surface app.* Alternatively, you can find the serial number via Command Prompt: 1. Type **CMD** in the search bar and press **Enter** to open a Command Prompt window. 2. Type the following command: - `console wmic bios get serialnumber` 3. The serial number will then be displayed within the Command Prompt window.
Unable to unenroll Surface Hub 2S from SEMM in order to roll back to Windows 10 Team	If the SEMM certificate becomes lost or corrupt, SEMM cannot be removed or reset on Surface devices. With this in mind, please ensure you have the appropriate backups of the certificate and its password.
In the Windows 10 Team OS, I used the Surface App to view additional device and accessory information, troubleshoot, and access support. Since the migration to Windows 10/11 Pro or Enterprise, this app is no longer installed.	The Surface App is not installed on Windows 10/11 Pro or Enterprise by default, but you can install it manually by following the steps here.
Does migrating my Surface Hub 2S device to Windows 10/11 Pro or Enterprise impact the standard or extended warranty for the device?	No, migrating to Windows 10/11 Pro or Enterprise does not change the warranty status of your Surface Hub 2S.

Version history

The following table summarizes changes to this article.

Version	Date	Description
v. 1.6	January 16, 2023	Added new section for troubleshooting and common problems
v. 1.5	December 1, 2021	Updated to show support for Windows 11

Version	Date	Description
v. 1.4	December 14, 2020	Provides further info about installing the MSI file for "Drivers and firmware for Windows 10 Pro and Enterprise OS on Surface Hub 2," advising that a second reboot may be necessary depending on the state of your system.
v. 1.3	December 3, 2020	Updated with guidance about managing SEMM enrollment.
v. 1.2	September 29, 2020	Miscellaneous updates that address usability feedback.
v. 1.1	September 15, 2020	Placed an additional note in the introduction that clarifies licensing requirements for installing a new OS.
v. 1.0	September 1, 2020	New article.

Configure Windows 10/11 Pro or Enterprise on Surface Hub 2

Article • 01/03/2023 • Applies to: Surface Hub 2S, Windows 10, Windows 11

After migrating to Windows 10/11 Pro or Enterprise, you can configure apps and settings to ensure the best experience using this personalized large screen touch and pen computer.

When performing these steps, you might find it helpful to use a wired or wireless keyboard and mouse.

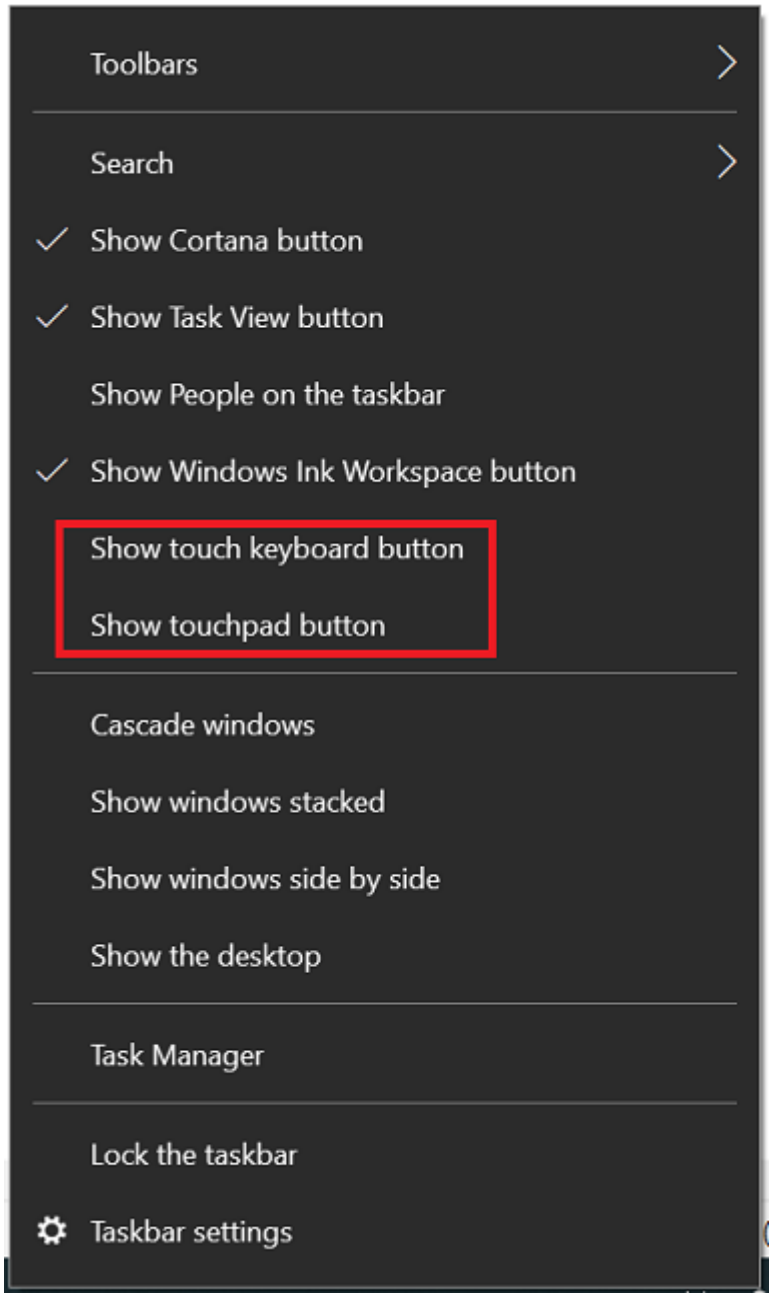
Configure system settings

1. Sign in with an account that has local administrator privileges on the device.
    - The user who performs the Azure AD join on Azure AD joined devices is automatically added to the local administrator group. Azure AD global administrators and Azure AD devices administrators are also local administrators.
    - You can type **net localgroup administrators** at a command prompt to list the accounts that have local administrator rights.
2. Rename the device using a friendly name, for example, **username-SHub-Desktop**.
3. Select **Start** > **Settings** > **Accounts** > **Sync your settings** and turn **Sync settings** off.
    - The settings used here are intended to enable the best large-screen touch experience, and therefore you may not want to sync other devices.
4. Restart the device.

Enable the touch keyboard and touchpad

1. Select **Start** > **Settings** > **Devices** > **Typing** and turn on **Show the touch keyboard when not in tablet mode and there's no keyboard attached**.
2. Tap and hold or right-click the taskbar and select the **Show touch keyboard button** and **Show touchpad button**.

- The touch keyboard is helpful for direct user input, and the virtual touchpad helps with precise selections, hovering screen tips, or as an alternative to tap and hold for right-click.
- See the following example.



3. Configure the touch keyboard to QWERTY and floating.

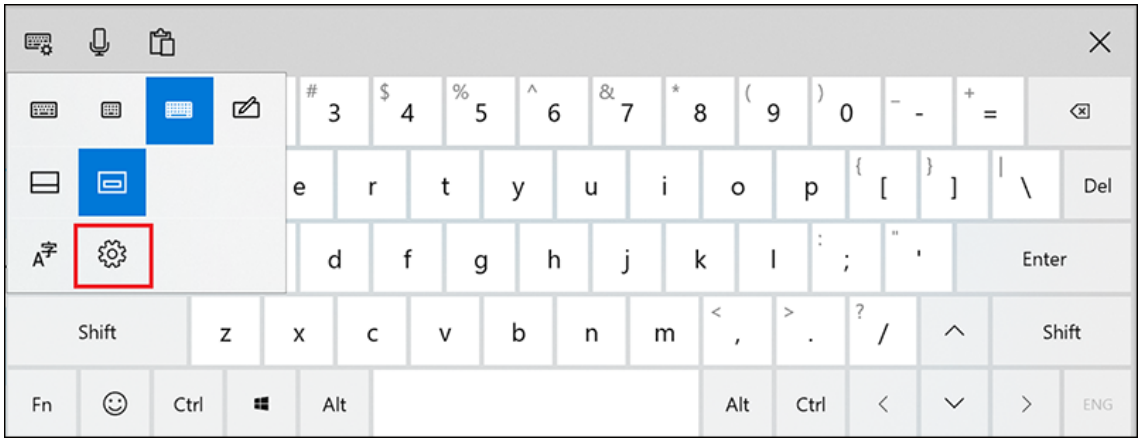
   a. Select the **Keyboard** icon on the taskbar to show the touch keyboard.

   b. On the touch keyboard, select the keyboard icon in the upper left corner to open keyboard settings.

   c. Select the next to last keyboard type on the top row to enable QWERTY and the last option on the second row to enable floating, which is helpful on this large screen. See the following examples.

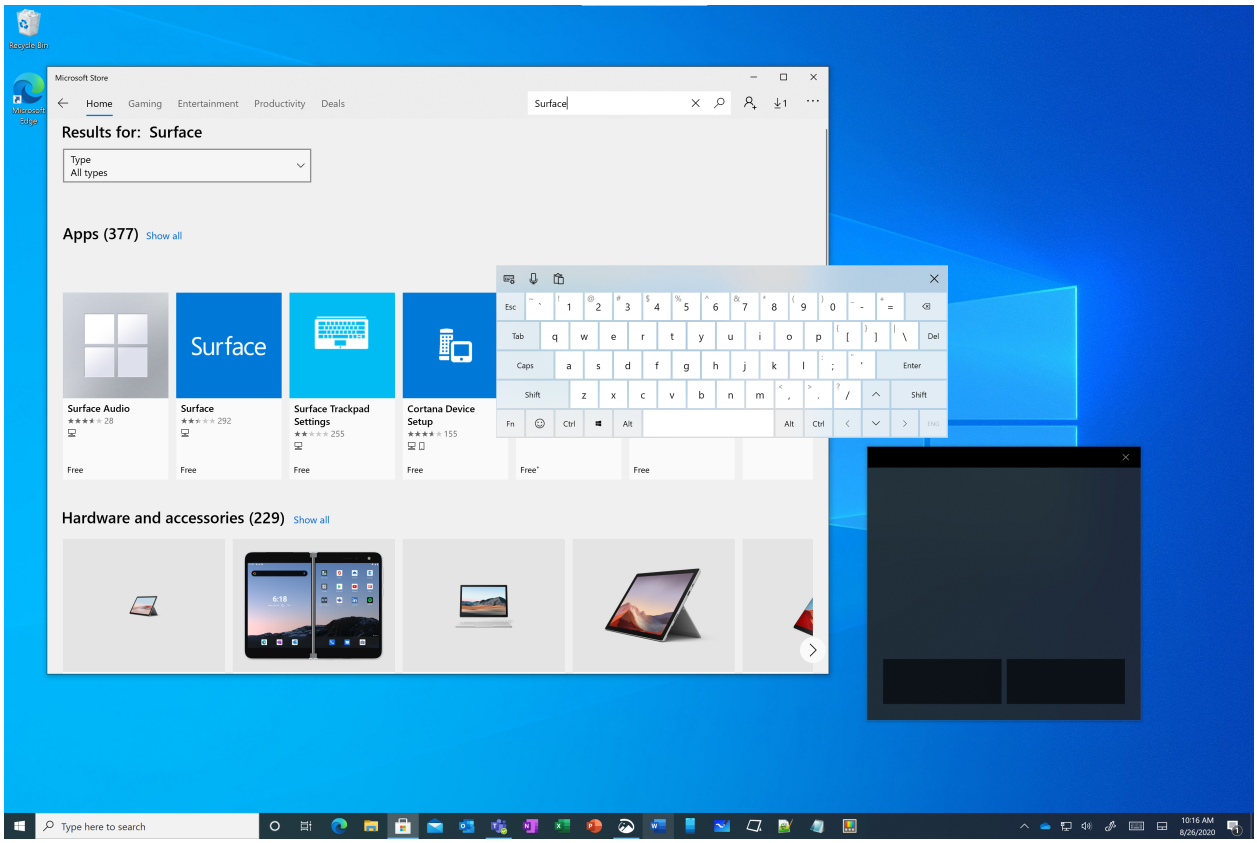
4. Configure the soft keyboard settings.

    a. Select the **Settings** icon on the touch keyboard or search for and open **Typing settings**.



    b. Enable all the options under Spelling, Typing, and Touch keyboard.

The following example shows the trackpad, which is useful to navigate and select options. The onscreen keyboard is being used to search the Microsoft Store:



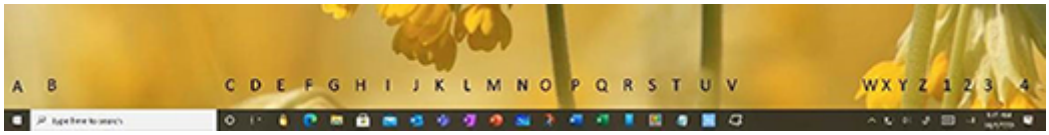
Configure Bluetooth keyboard and mouse (optional)

Connect a keyboard and mouse if you use the device as your primary Windows device, or you often use it for typing or precision work.

If your Surface Hub device is near a PC, you can use Mouse without Borders to move seamlessly between the Surface Hub and the PC. For more information, see Microsoft download from The Garage: Mouse without Borders.

Example of Taskbar layout

After completing the below steps to set up/configure your Surface Hub 2 for Windows 10/11 Pro or Enterprise, we recommend you utilize pinning your most-used applications to the Taskbar for a quick one-touch launch of each application. Below is an example of what your taskbar could look like:



Update installed apps

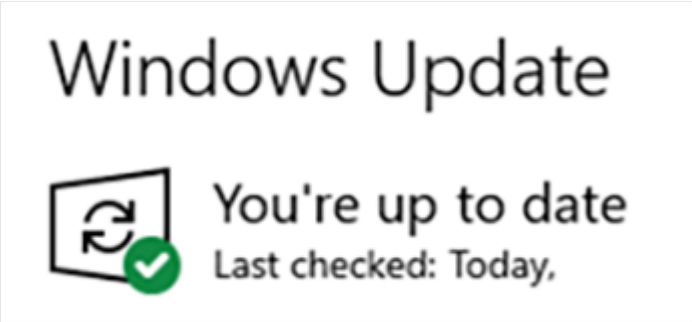
To update all installed Store apps:

1. Open the Microsoft Store app and select the **See more** ellipsis in the top-right corner.
2. Select **Downloads and updates.**
3. Select **Get updates**

Scan for and install all Windows Updates

After migration, there may be servicing and feature updates available for you to install.

- Go to **Settings** > **Update & Security** > and select **Check for updates**.
- If there are any updates, install them, reboot, and then repeat the process until you see the following notification:



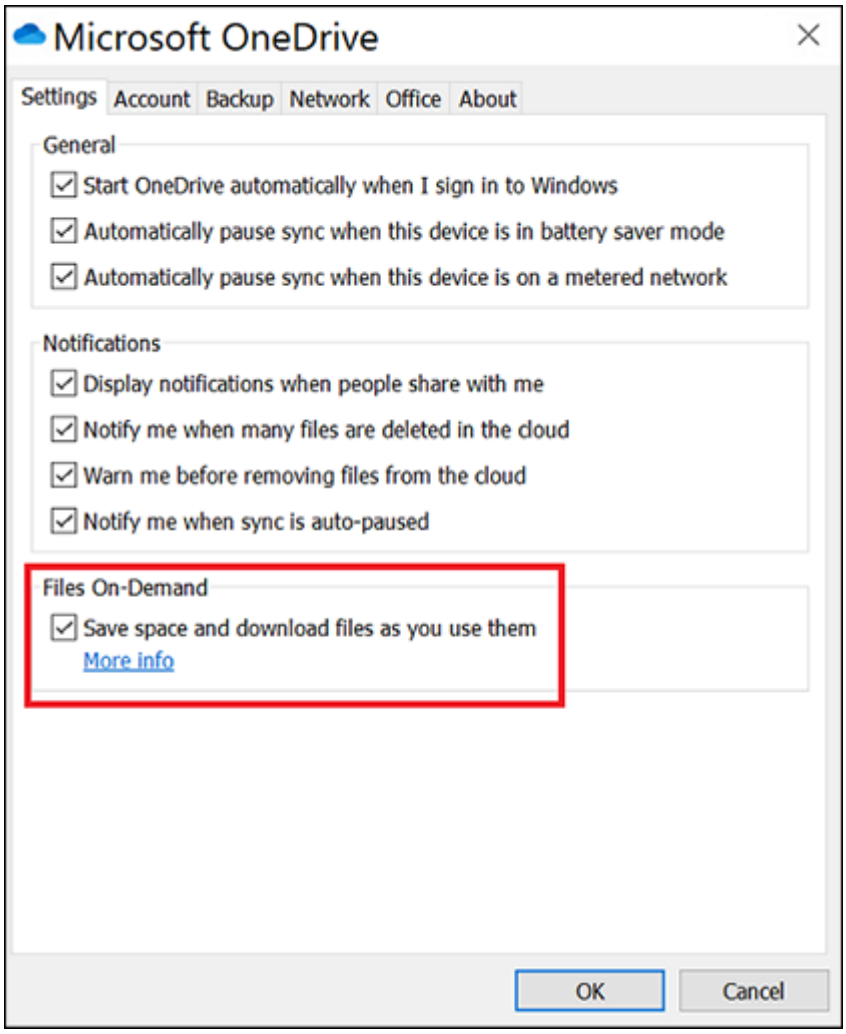
OneDrive for Business

Use OneDrive for Business to easily share tools, logs, and other files between all your work devices.

- OneDrive lets you share your work files between your laptops, Surface Hub Desktop, and your Intune-managed mobile devices. Files can be edited on any device, and all network-connected devices will be updated with the changes.

- Considering the size of the Surface Hub SSD (128GB), if you configure OneDrive on your Surface Hub Desktop device, make sure the default configuration is to keep the files online and download files as you use them.

To configure OneDrive to download files only when needed, set the **Files On-Demand** setting to **Save space and download files as you use them**. For more information, see Query and set Files On-Demand states in Windows.



> ⓘ Note
>
> You can also repeat these steps to configure a personal OneDrive but be sure to conserve drive space and only download files as you need them.

SharePoint and Teams

SharePoint and Teams Channel files can also sync locally to your desktop devices, such as laptops and Surface Hubs, using the OneDrive sync engine.

To sync internal corporate files to your local drive with the OneDrive sync app:

1. Go to a SharePoint site and navigate to the top-level document directory for files you are interested in viewing or editing from your local device.
2. Select on the **Sync** button on the top of the SharePoint ribbon.
3. Select on **Open** on the popup **This site is trying to open Microsoft OneDrive**.

4. Verify that the SharePoint files are synchronizing to your local drive by selecting the OneDrive icon at the bottom right of the taskbar.

5. Verify the configuration is set to keep the files online and download the files only as you use them:

   a. Open file explorer.

   b. Navigate to and right-click your SharePoint name; for example, **Contoso \ <SharePoint Document Folder Name>**.

   c. Select **Free up space**.

   d. The Status column will display the status of files and folders. For more information, see Sync SharePoint files with the OneDrive sync client.

6. Teams Channel files are stored in SharePoint sites, with the same SharePoint document functionality, including version history and synchronizing to your local desktop devices. To sync Teams Channel files:

   a. Navigate to the Teams Channel of interest and select the **Files** tab at the top. Then select **Sync**. The files will start synchronizing and be visible in File Explorer at **Desktop \ Contoso \ <name of the Teams Channel>**.

   b. Use the same procedure you used for synchronizing SharePoint sites to keep the files in the cloud and only download them when you use them, by tap and hold or right-click in File Explorer on the Teams Channel name, and then selecting **Free up space**.

Surface Hub pen settings

Pair the Bluetooth Surface Hub Pen

Pair the pen to keep the pen firmware up to date, set the pen shortcuts, and get battery charge information on the Bluetooth device settings page, or in the Surface app:

1. Select **Start** > **Settings** > **Devices**.

2. Select **Add Bluetooth or other device**.

3. Choose **Bluetooth**.

4. Remove the pen tail button and shake to disconnect the battery connection.

5. Put the cap back on and press and hold the cap until the pairing LED flashes.

6. On the Surface Hub Bluetooth settings, choose **Surface Hub 2 Pen**.

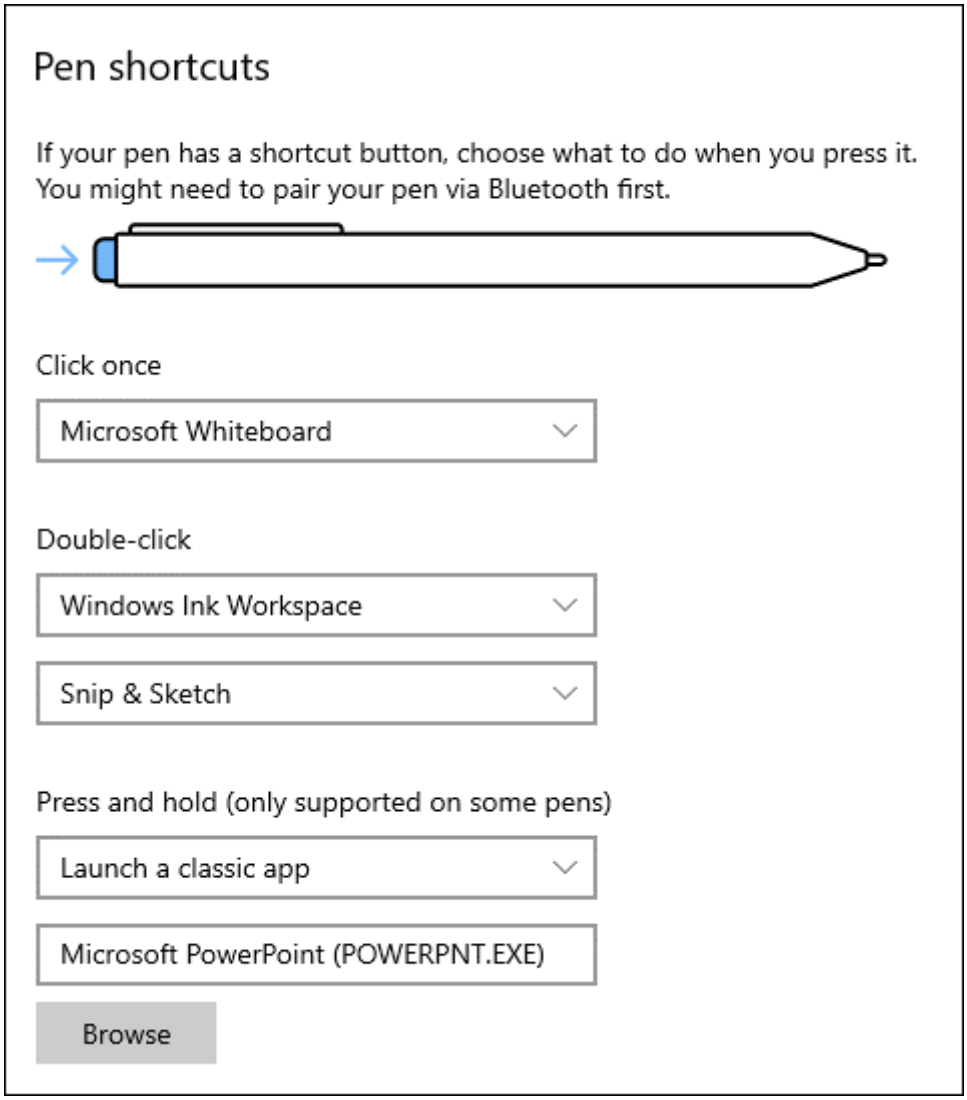
7. Complete the pairing operation.

8. If the pairing is not successful, try to pair the pen again. If that doesn't work, you can test to see if the battery is charged by verifying the pen works in the Whiteboard application. If not, replace the battery and try to pair the pen again. If necessary, restart the device and then try again.

Set pen shortcuts The Surface Hub pen has a shortcut button sometimes called a "tail click." Configuring shortcuts requires you to first pair the pen, as described earlier.

1. Search for Pen and select **Pen & Windows Ink settings**.

2. Near the bottom of the page, select Pen shortcuts which opens the dialog box, shown here:



Camera configuration

You can mount the camera on the top or either side of the device. Mount the camera in a position to optimize the camera angle if you are using the Hub with a desktop stand instead of a cart, or are near the Hub. The camera does not auto-rotate, so you need to have a 2mm hex key to manually rotate the camera.

For more information on how to side-mount the camera and rotate the camera manually, see Surface Hub 2S camera lens orientation.

Windows Hello configuration

Surface Hub 2S running Windows 10/11 Pro or Enterprise allows the full suite of Win32 desktop applications as well as biometric Windows Hello options. The Surface Hub 2 Fingerprint Reader accessory can be plugged into any USB-C port on the device.

To order a Surface Hub 2 Fingerprint Reader or view technical specs, see (surface-hub-2-essential-add-ons.md" target="_blank">Essential add-ons for Windows 10 Pro and Enterprise on Surface Hub 2 .

After inserting the fingerprint reader, select **Start** > **Settings** > **Accounts** > **Sign-in options** > **Windows Hello Fingerprint** to enroll your fingerprint.

Use a Windows Hello certified device for face recognition. The Surface Hub 2S camera does not support Windows Hello face recognition.

Enable a Lock Screen shortcut icon on the taskbar

To add an icon to the taskbar that enables one-touch screen lock similar to the Windows-L keyboard shortcut:

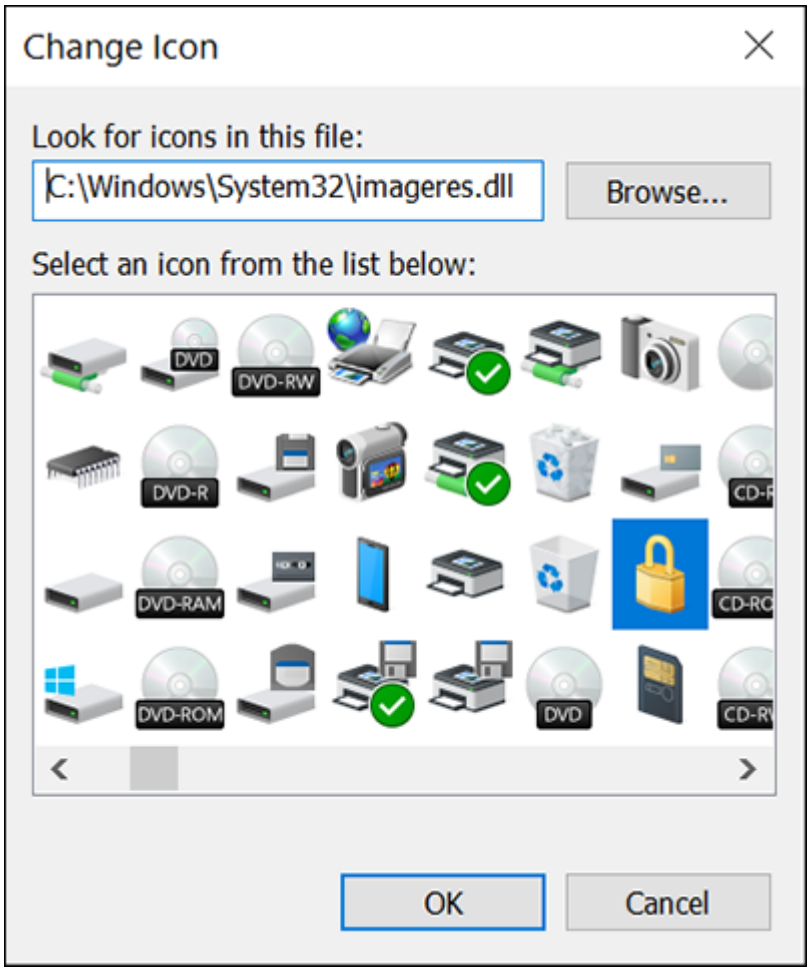
1. Tap and hold or right-click on the desktop, select **New** > **Shortcut** > **Browse** > **Desktop** > **OK** > **Next**.

2. Provide a name for the shortcut such as **Lock my PC**, and then select **Finish**.

3. Right-click or tap and hold the newly created shortcut on the desktop, and select **Properties**. On the **Shortcut** tab, enter the following in the **Target** field: **Rundll32.exe User32.dll,LockWorkStation**

4. Select the **Change Icon** button and browse to **C:\Windows\System32\imageres.dll** and select an icon to use.

   See the following example:



5. Select **OK** to save the shortcut.
6. Right-click or tap and hold the shortcut and select **Pin to taskbar**.
7. After you have pinned the lock shortcut to the taskbar, you can delete it from the desktop.

Applications

Microsoft Whiteboard

To install the Microsoft Whiteboard:

- Select the **Windows Ink Workspace** icon on the lower right of the taskbar and download **Whiteboard**.

Alternatively, you can install Whiteboard from the Microsoft Store:

1. Open Microsoft Store app and search for **Whiteboard**.

2. Choose **No thanks** to sign in and use across devices.
3. Pin Whiteboard to the taskbar.

Surface app

1. In the Microsoft Store, search for **Surface**.
2. Set the **Available on** filter to **All devices**.
3. Install the **Surface** app. This should be the first app listed. You might need to associate your MSA to the Store in order to install the app.
4. Pin the **Surface** app to taskbar.

Snip & Sketch

1. Open the **Snip & Sketch** app and pin it to the taskbar.
2. Select the ellipsis in the upper right corner and then select **Settings**.
3. In **Settings**, turn on **Auto copy to clipboard**, **Save snips**, and **Multiple windows** (optional).

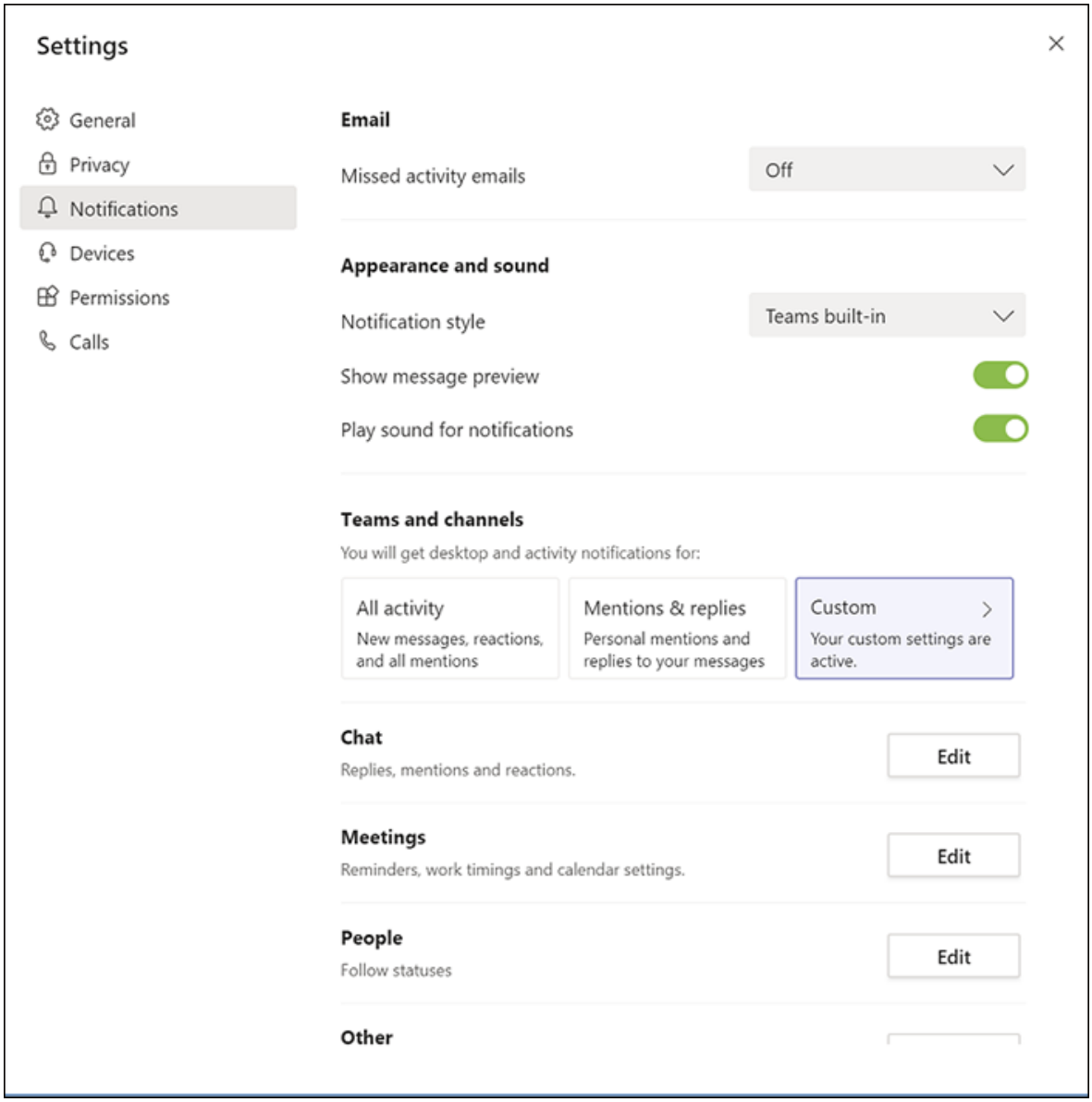
Microsoft Office

1. Open the Office Portal and install your desired applications.
2. Pin desired Office applications to the taskbar.
3. If Outlook is installed, be sure to set the Outlook OST to only save last two weeks cache. This will vastly reduce disk usage and setup time.
    - Select **File** > **Account Settings** and select your account.
    - Select **Change** and set the slider for **Use Cached Exchange Mode** to 14 days.

Microsoft Teams

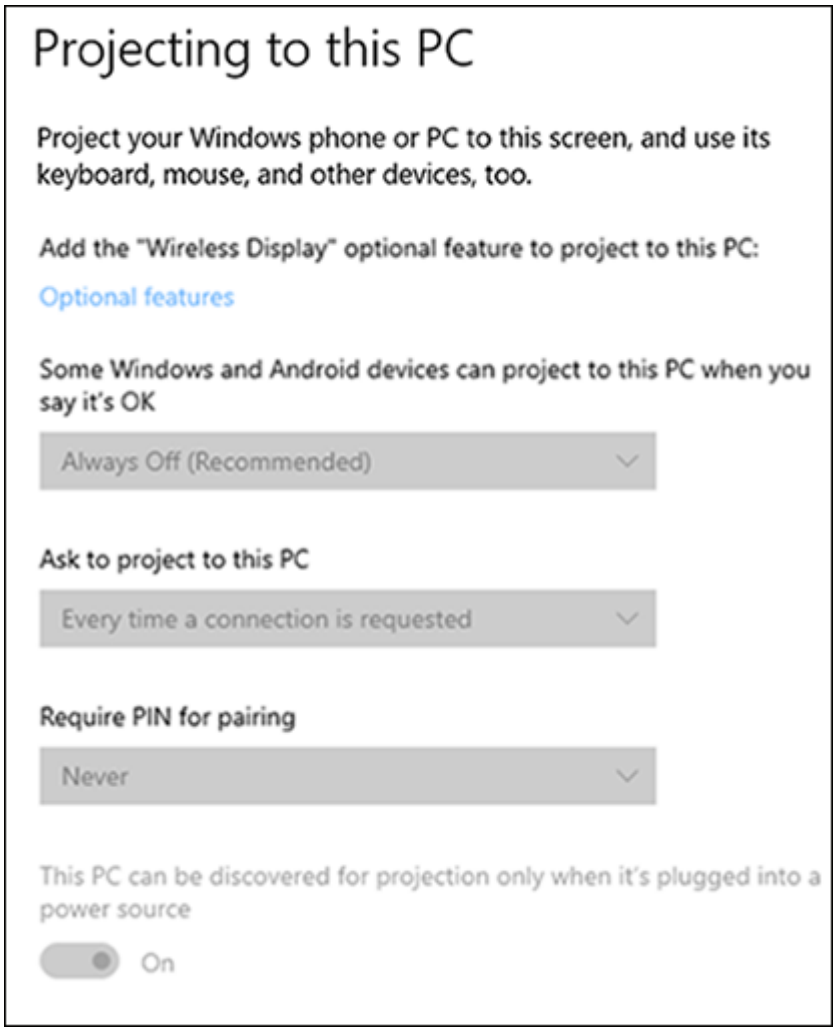
1. Download and install Microsoft Teams.
2. Configure settings to Auto-start application (optional).
3. Pin Teams to the taskbar.

4. Consider reducing Teams notifications on the device to avoid distractions (optional).



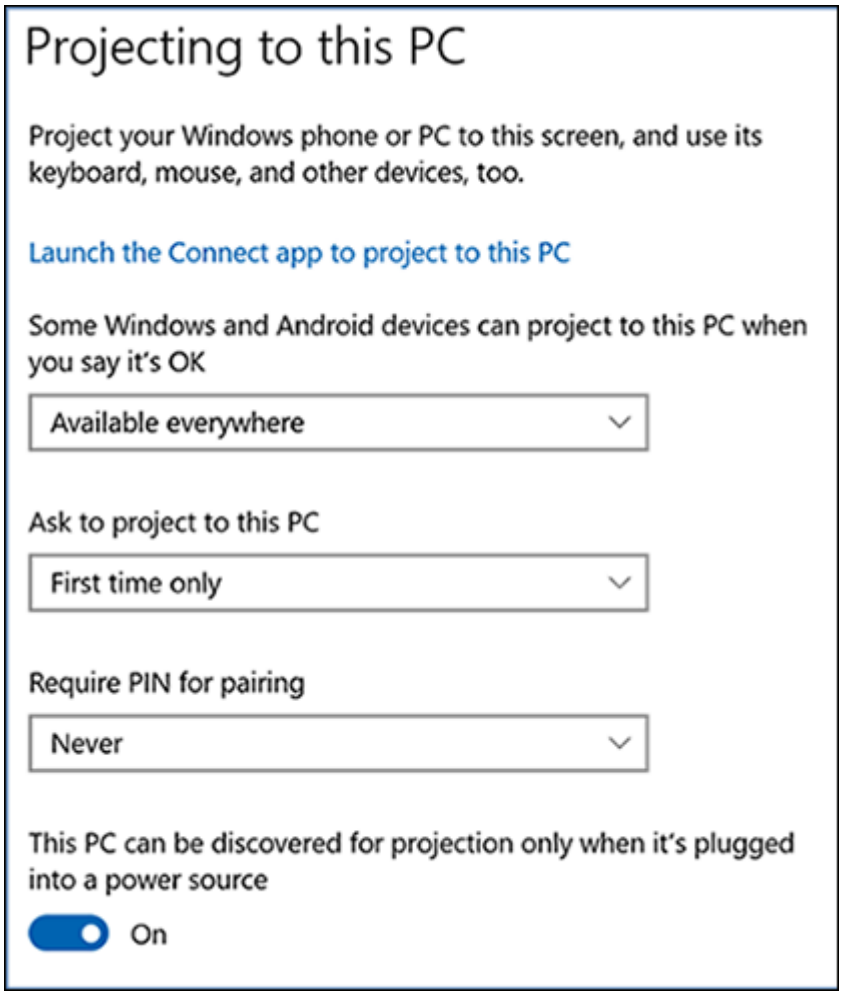
Connect app

> **ⓘ Important**
>
> In Windows 10, version 2004 and later, the Connect app for wireless projection using Miracast is not installed by default, but is available as an optional feature. If you have installed (or updated to) Windows version 2004 or later, you may see the following on the Projecting to this PC screen in settings:

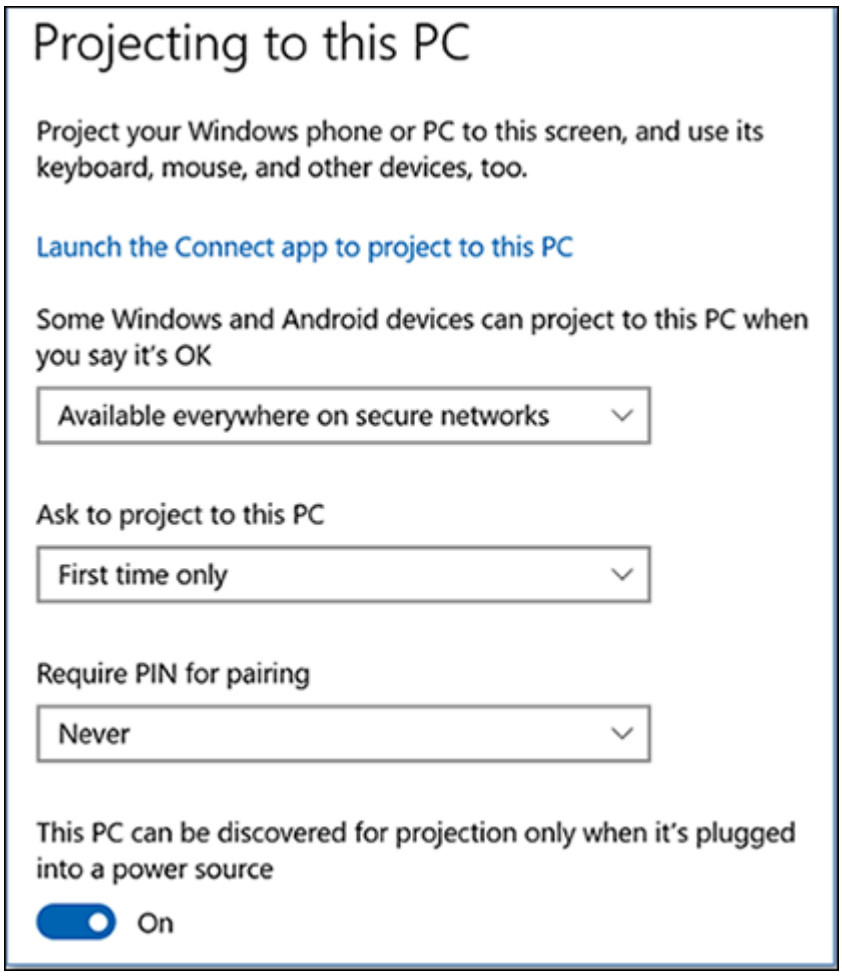


1. To install the app from the "Projecting to this PC" settings page, select **Optional features** > **Add a feature** and then install the **Wireless Display** app.
2. Under **Some Windows and Android devices can project to this PC when you say it's OK**, choose:
    - **Available everywhere** if the device is not on a corporate network.
    - Otherwise, choose **Available everywhere on secure networks**.
3. Under **Ask to project to this PC**, choose **First time only**.
4. Under **Require PIN for pairing**, choose **Never**.
5. To then launch the app and pin it to the taskbar, search for **Connect**.
6. Open the app. While the app is open, right-click on the Connect app icon on the taskbar, and select **pin to taskbar**.
7. Then close the Connect app. **Project to this PC** might not work unless the app has been run at least once.

Recommended configuration when not on the corporate network:



Recommended configuration on the corporate network:



Your Phone

The **Your Phone** app is installed by default on Windows 10. If it is not present, you can also install it from the Windows Store.

For information about setting up the app, see How to set up Your Phone on Windows 10 and sync data between your PC and phone. Also see How to fix common problems with Your Phone app on Windows 10.

Fancy Zones

Fancy Zones is part of a collection of tools called PowerToys on GitHub.. It is a great way to utilize the screen real-estate on a Surface Hub 2 by giving you the ability to define fixed layouts on your display ("zones"), and then select which app will then run in each zone.

The PowerToys wiki has instructions for how to use and customize each tool, including FancyZones. At a high level – after installing PowerToys, you can select or create a custom layout, and then hold the shift key down and drag or use keyboard keys to move a running app into specific zones. Using a Bluetooth or USB keyboard and mouse will help with this, or you can use the on-screen touch keyboard and touchpad.

Power toys tips

- To receive email notifications of PowerToys release updates on GitHub, click the "sign-up" button at the top of the page.
- Once PowerToys is installed, you can receive Windows notifications and/or download and install the latest updates by configuring the PowerToys settings **Download updates automatically** to on.
- To get to the PowerToys settings, select the up carat **Running apps** on the taskbar, and then right-click or press and hold the PowerToys icon until the menu appears. Select "Settings".
- At the bottom of the PowerToys settings page, turn **Download updates automatically** to on.
- When an update has been released, a Windows notification will appear giving you the option of when to install the update.

Edge Chromium browser

Download and install the new Edge Chromium browser.

Surface Hub Hardware Diagnostic tool

The Surface Hub Hardware Diagnostic tool available for free from the Microsoft Store. The tool is designed to help you make sure your Surface Hub is performing at its best. It contains tests to determine if your firmware is up to date and configured correctly. Interactive tests allow you to confirm essential functionality is working as expected. If problems are encountered, results can be saved and shared with the Surface Hub Support Team. Click on the link to install it from the Microsoft Store, and then pin the application to your taskbar.

Additional settings

Pen tail select to launch Whiteboard

1. Search for **Pen** and select **Pen & Windows Ink settings**.
2. Near the bottom of the page, under **Pen shortcuts** set **Select once** to **Microsoft Whiteboard**.

Power management

There are several power settings available to get the best experience using Windows 10/11 Pro or Enterprise on Surface Hub 2. This includes screen and pc timeouts and how they interact with the built-in human presence detection (Doppler), the screen saver and password protection, and then if appropriate how to by-pass group policy power settings intended for laptop / desktop users.

Windows 10/11 Pro or Enterprise on Surface Hub 2 keeps the screen from going to sleep by touch, mouse, and keyboard actions, as well as the built-in human occupancy detection (Doppler). Human occupancy detection is enabled by default, but if desired it can be disabled in UEFI by toggling the device option in the Surface UEFI Configurator tool either as part of the initial migration, or by building and applying a later UEFI configuration package.

Power Management: Screen and PC sleep settings

1. Select **Start** > **Settings** > **System** > **Power & sleep**.
2. Set the power mode slider to **Best performance**.
3. Configure screen and sleep values to your preference while also accounting for Doppler presence detection that wakes up the device when movement is detected. Accordingly, as a best practice, it's recommended to set Screen to **Turn off after 2 hours** and the PC to **Turn off after 4 hours.**

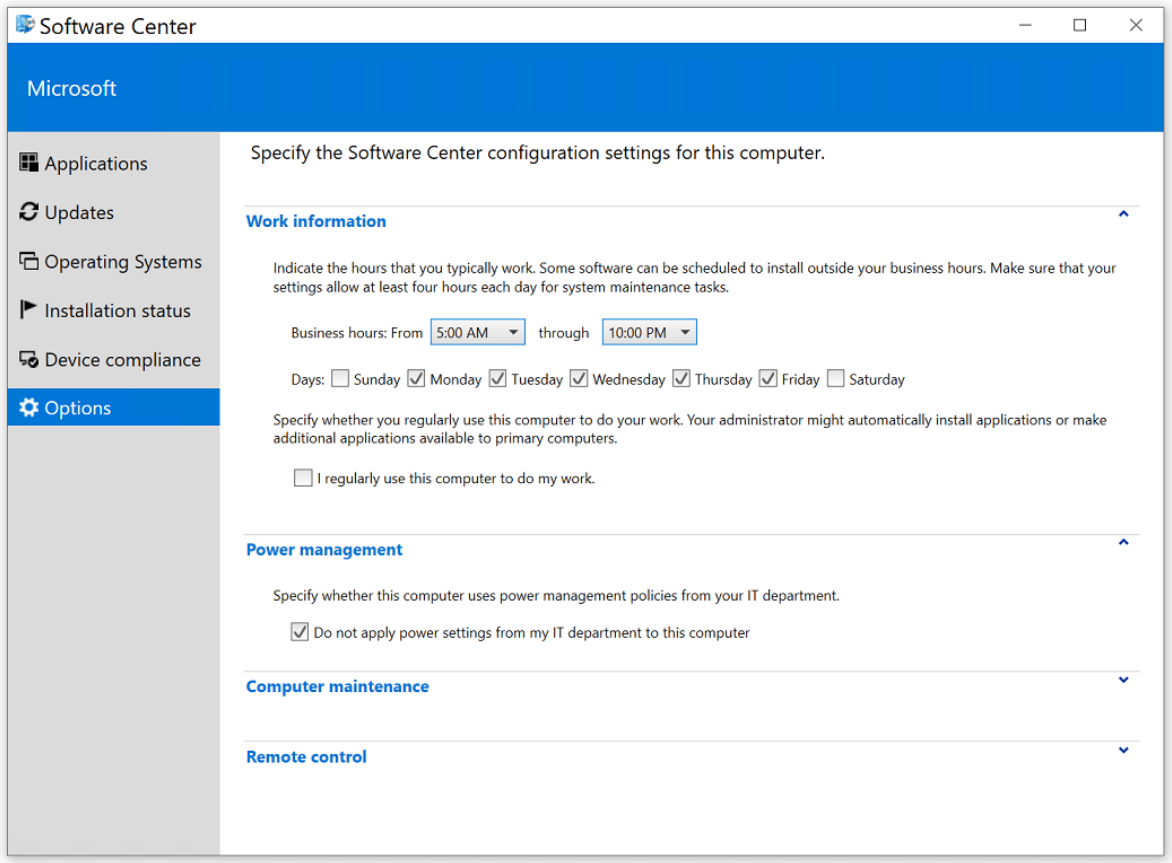
Power Management: Screen saver

1. Search for **Lock Screen** and open **Lock screen settings**.
2. Configure **Screen timeout settings** and **Screen saver settings** to your preference. Recommended default values are:
    - Screen saver to (None) or a screen saver of your choice.
    - Wait time to 15 minutes.
    - On resume, display logon screen.

Power Management: Group Policy

Before performing the following procedure, check with your IT department for approval to exclude a Surface Hub 2S device from global power management policy. Some power management settings can disable the presence detection function.

1. Search for **Software Center** and open it.
2. Select **Options**.
3. Expand the **Power management** and select **Do not apply power settings from my IT department to this computer**.



Storage Sense

The Surface Hub 2 has a 128GB SSD for local storage, so it is necessary to consider the use of storage saving measures during normal usage. To configure Storage Sense:

1. Search for **storage settings**, which is found under **System settings**.
2. Under **Settings**, select **Turn on storage sense** to open the **Storage** settings page.
3. Turn Storage Sense to **On**.
4. Select **Configure Storage Sense or run it now** and configure settings to keep files online as much as possible (due to limited drive space).

Recommended settings:

- Run Storage Sense = Every Day.
- Delete temporary files that my apps aren't using = Every 14 days (at least).
- Delete files in my Downloads folder if they have been there for over = 30 days.
- OneDrive: Content will become online-only if not opened for more than = 30 days.

Tablet mode

Turn on Tablet mode if desired for accessibility needs.

Sound settings

1. Search for **Sounds settings** and open this page.
2. Select **Sound Control Panel** on the right and select the **Sounds** tab.
3. Under **Program Events** set **Device Connect** and **Device Disconnect** to **None**.

Silence notifications

1. Search for **Focus assist** and open this page.
2. Select **Alarms Only**. This will avoid constant notification flyouts.

Disk Cleanup

1. Search for **Disk Cleanup** and open this app.
2. Under **Files to delete**, select the files you wish to delete.
3. Also select **Clean up system files**.

Complete and verify

1. Scan for and install all Windows Updates.
2. Update Group Policy.
   a. At an elevated command prompt, enter **gpupdate /force /boot /wait:0**.
3. Restart the device.
4. Verify taskbar apps.
   - Connect App
   - Lock Icon
   - Snip & Sketch
   - Teams (if applicable)
   - Office Apps (if applicable)
   - Surface App
   - Whiteboard
5. Verify presence detection.
   - Presence detection will be a green icon in the system tray.
6. Verify projecting to this PC is enabled with the Connect App. After configuring **Project to this PC** settings, run the Connect App at least once. (Subsequently, the Connect App does not need to be running in order to project to Surface Hub.)
7. Verify power and sleep settings.
   - Screen Saver: 15 minutes, set to (none), Mystify or Blank; ensure the check box for requiring password is selected.
   - Screen: **Turn off after 2 hours**.
   - PC: **Turn off after 4 hours**.
8. Verify Windows Hello is working.
9. Verify sync your settings is disabled.
10. Verify startup apps.

> **Tip**
>
> After installing and configuring Windows 10, the Surface Hub 2S can be managed just like any other Windows 10 or Windows 11 device.

Related topics

Migrate to Windows 10/11 Pro or Enterprise on Surface Hub 2

Essential add-ons for Windows 10/11 Pro and Enterprise on Surface Hub 2

Article • 01/03/2023

If you have migrated from Windows 10 Team to Windows 10 or Windows 11 Pro or Enterprise on Surface Hub 2, you can choose from a wide variety of accessories that connect via USB-C, USB-A, HDMI, or Bluetooth.

Surface Hub 2 Fingerprint Reader

If you're running Windows 10/11 Pro or Windows 10/11 Enterprise on Surface Hub 2, you can sign in using the optional Surface Hub 2 Fingerprint Reader, a biometric authentication option that uses Windows Hello.

Ordering

Commercial customers can place orders through their Surface Authorized Device Resellers.

To use Surface Hub 2 Fingerprint Reader:

1. Insert the fingerprint reader into any of the USB C bezel ports, located on each side of the device.
2. **Go to Start** > **Settings** > **Accounts** > **Sign-in options** > **Windows Hello Fingerprint** to enroll your fingerprint.

For more information about configuring the fingerprint reader to sign in using Windows Hello, see the following:

- Learn about Windows Hello and set it up
- Windows Hello biometrics in the enterprise.

Table 1. Surface Hub 2 Fingerprint Reader tech specs

Component	Description
USB	Customized USB Type-C
System requirement	Windows 10/11 Pro, Windows 10/11 Enterprise.

Component	Description
Windows certification	Windows 10/11
False Acceptance Rate (FAR)	1/1.5 million. FAR shows the probability of a biometric security system to incorrectly accept access attempts by unauthorized users.
False Rejection Rate (FRR)	4.9%. FRR shows the probability of a biometric security system to incorrectly reject access attempts by authorized users.

> **Note**
>
> Windows 10 Team, which runs on Surface Hub 2S does not support the Surface Hub 2 Fingerprint Reader. This is because Windows 10 Team is designed to allow multiple users to interact with the device in a conference room environment.

Windows Hello face recognition

Windows 10/11 Pro and Enterprise on Surface Hub 2 supports Windows Hello for authentication and requires a Windows Hello certified camera accessory. Note that the built-in camera for Surface Hub 2S is not designed for authentication and does not support Windows Hello. For more information, see Windows Hello.

Audio and video accessories

You can extend the audio and video capabilities of Surface Hub 2 with audio and camera peripherals using the USB-C or USB-A ports.

For information about recommended accessories, see:

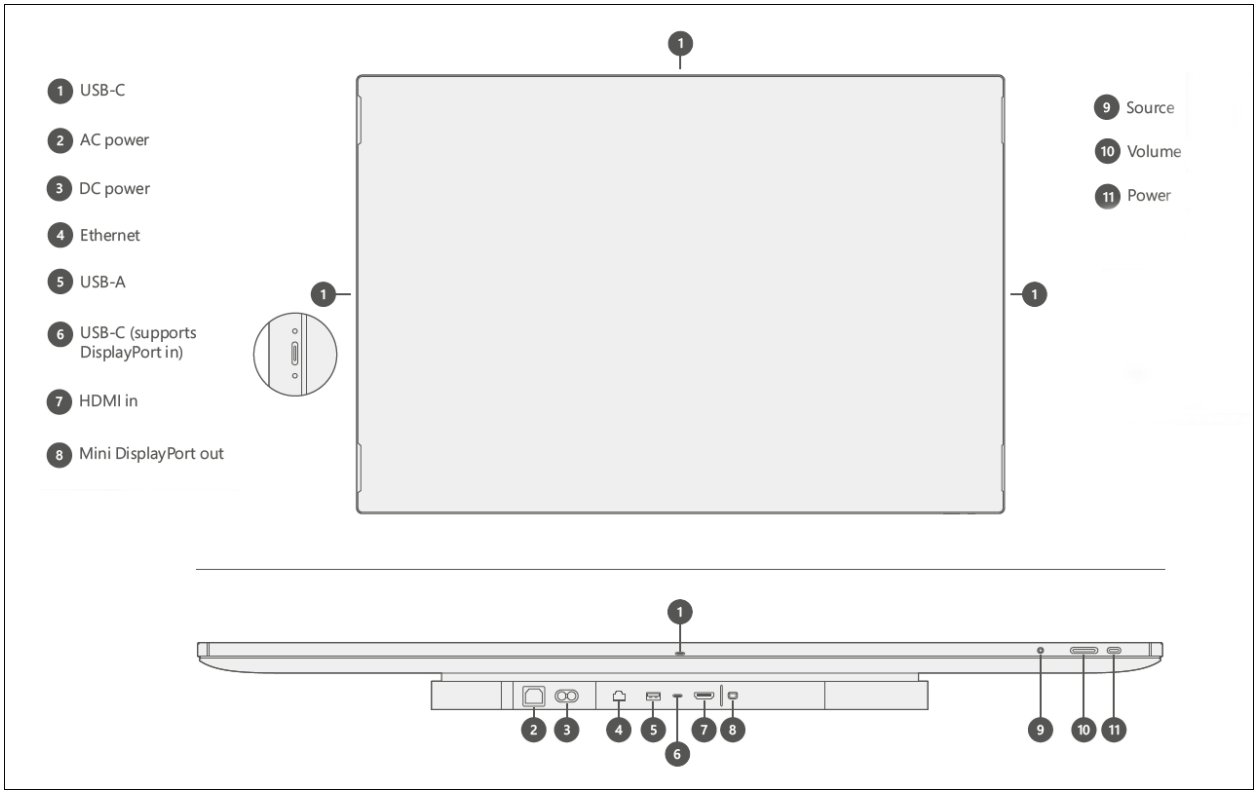
- USB audio and video devices certified for Microsoft Teams
- IP Phones certified for Microsoft Teams

Other accessories

Surface Hub 2 includes the following ports for connecting a wide variety of devices.

- 1 x USB A port on compute module (behind display)
- 4 x USB C ports on bezels
- Bluetooth 4.1 support

- HDMI 2.0



For more information, see Surface Hub 2S ports and keypad overview

Learn more

- Configure Windows 10/11 Pro or Enterprise on Surface Hub 2.

What's new in Windows 10 Team 2020 updates

Article • 03/21/2023

Surface Hub benefits from periodic updates that deliver new features and functionality. The 2020 Update (20H2) to Windows 10 Team, and subsequently Update 1 & Update 2, deliver significant improvements to device deployment and manageability along with the latest Windows features.

Windows 10 Team 2020 Update 2

Display and preferred language support

After a Surface Hub admin installs additional languages, end users can change the display language by selecting a new one from the available installed languages. Ensure that your Surface Hub has KB5023773 (or a subsequent Windows update) installed. To learn more about the latest Windows 10 Team updates, refer to Surface Hub update history.

GCC High support

After installation of this update (KB5010415 or a subsequent Windows CU), Surface Hubs are supported in GCC High environments. At this time, additional steps are needed for the Teams Rooms client to successfully connect to GCC High tenants.

Support for Surface Hub 2 Smart Camera

The AI-powered Surface Hub 2 Smart Camera is optimized for hybrid teams allowing remote participants to see people interact with content on the Surface Hub while also viewing everyone else in the room. To learn more, see Install and manage Surface Hub 2 Smart Camera.

Support for Progressive Web Apps (PWAs)

Admins can remotely install PWAs on Surface Hubs using a mobile device management provider (MDM) applying a provisioning pack. To learn more, see Install Progressive Web Apps on Surface Hub.

Ease of Access updates

Users can adjust Ease of Access settings during a Surface Hub session and close apps just like they do in other versions of Windows 10 or Windows 11.

- **Ease of Access**. Users can adjust the following settings without signing in: Display, Text cursor, Magnifier, High contrast, Narrator, Closed captions, and Keyboard.
- **Familiar UI for apps**. Users can close apps on Surface Hub by selecting the Close button in the top right corner of the app. This removes the need to close apps by dragging them to the bottom of the Surface Hub display. (Note: This functionality will be available on the Edge browser as part of the next Edge update, scheduled for March 2022.)

To learn more, see Adjust Ease of Access settings on Surface Hub.

Administrator updates

- **Event Viewer**. Admins can access the Windows Event Viewer directly from the Settings app.
- **New mobile device management (MDM) policy settings**. New Configuration service providers (CSPs) include:
  - TimeLanguageSettings-CSP
  - LocalUsersAndGroups-CSP

To learn more, see Configure non-Global Admin accounts on Surface Hub.

Windows 10 Team 2020 Update 1

Support for new Teams Rooms application

After installation of this update (KB5005101 or a subsequent Windows CU), Surface Hubs support an automatic upgrade to the new Teams Rooms client through Windows Update.

Support for new Whiteboard application

After installation of this update, Surface Hubs support an automatic upgrade (when available) to the new Whiteboard app through Microsoft Store updates.

New Microsoft Edge browser installed by default

After installation of this update, Surface Hubs will automatically replace their Microsoft Edge Legacy browser with the new Chromium-based Edge browser. To learn more, see Manage Microsoft Edge on Surface Hub. Edge Legacy is no longer available on Windows 10 Team after installation of this update or a subsequent Windows CU.

Windows 10 Team 2020 Update (20H2)

Deployment and manageability

- **Modern authentication for cloud device accounts**. Surface Hub supports Exchange Web Services (EWS) and Active Directory Authentication Library (ADAL) based authentication to connect to Exchange, allowing customers to deprecate the use of Basic authentication. To learn more, see Modern authentication on Surface Hub.

- **More than 20 new and updated MDM policy settings**. These policy settings give IT admins improved control over multiple device settings, including app updates from the Microsoft Store, wireless projection settings such as Miracast over infrastructure, network settings such as Quality-Of-Service and 802.1x wired authentication, and new privacy/GDPR related settings. New CSPs include:
  - Accounts CSP
  - Firewall-CSP
  - RemoteWipe CSP
  - Wifi-CSP
  - Wirednetwork-CSP

To learn more, see:

- CSPs supported in Microsoft Surface Hub
- Manage Surface Hub with an MDM provider

Azure Active Directory Joined devices

- **Single sign-on (SSO) for Azure AD joined devices**. When users sign in with their Microsoft 365 credentials to **My meetings and files**, their credentials flow seamlessly from app to app – including Microsoft 365 experiences in the browser.
- **Conditional access (CA) for Azure AD joined devices**. IT admins can control user access to organizational resources from Azure AD joined Surface Hubs by assigning device policies per their corporate security and compliance requirements.

- **Support for non-Global admins for Azure AD joined devices**. Customers can choose a more granular set of admins within their admin hierarchy to manage Surface Hub. To learn more, see Configure non-Global Admin accounts on Surface Hub.

Inking improvements

- **Support for dual-pen inking on Surface Hub 2S**. Use the whiteboard and collaborate side-by-side on Surface Hub 2S with two Surface Hub 2 Pens. Any system hardware update installed after upgrading to Windows 10 Team 2020 will add firmware support for this scenario.

Microsoft Teams

- **Microsoft Teams installed by default**. Microsoft Teams is the default app for meetings, calls and collaboration on new Surface Hub devices, which can be changed or configured via MDM or directly on Surface Hub using the Settings app. To learn more, see Deploy Microsoft Teams.

- **Support for Proximity Join with Microsoft Teams**. Proximity Join lets users take scheduled Microsoft Teams calls on a nearby Surface Hub using their laptop or phone. It also lets users transition an in-progress meeting to a nearby Surface Hub. Windows 10 Team 2020 Update adds Mobile Device Management (MDM) support to configure Proximity Join. To learn more, see:
  - Microsoft Teams Blog.
  - Manage Microsoft Teams settings on Surface Hub

- **Support for Coordinated Meetings with Microsoft Teams**. In meeting rooms that feature a Surface Hub and a Microsoft Teams Room device, or spaces with two Surface Hub devices, Coordinated Meetings let users quickly leverage both devices during a Microsoft Teams meeting. Users can join a meeting from either device with a single tap and maximize screen real estate by showing video feeds on one device and a digital whiteboard or content on the other. Windows 10 Team 2020 Update adds Mobile Device Management (MDM) support to configure Coordinated Meetings, and the feature will be subsequently released as a Microsoft Teams update through Microsoft Store. To learn more, see Set up Coordinated Meetings with Microsoft Teams Rooms and Surface Hub.

Security

- **Passwordless sign-in using FIDO2 security keys** With FIDO2 security keys, users can quickly sign in to Surface Hub without typing usernames and passwords. Combined with Single Sign-On (SSO), this feature provides fast and seamless authentication to files, apps, and websites during a meeting. To learn more, see Configure passwordless sign-in on Surface Hub.
- **Improvements to passwordless sign-in using Microsoft Authenticator**. For organizations that use Azure AD, users can sign in with the Microsoft Authenticator app. Additionally, users can sign in with their preferred email aliases in Azure AD or their User Principal Name (UPN). To learn more, see Sign in to Surface Hub with Microsoft Authenticator.

Learn more

- Surface Hub update history.
- Windows 10 Team 2020 Update 1 released to all Surface Hubs
- Windows 10 Team 2020 Update available October 27

Operating system essentials for Surface Hub

Article • 03/27/2023 • Applies to: Surface Hub, Surface Hub 2S

The Surface Hub operating system, Windows 10 Team, originated with Windows 10 Enterprise, providing rich support for enterprise management, security, and other features. However, there are important differences between them. While the Enterprise edition is designed for PCs, Windows 10 Team is designed from the ground up for large screens and meeting rooms. When you evaluate security and management requirements for Surface Hub, it's recommended to consider it as a new operating system. This article highlights the key differences between Windows 10 Team on Surface Hub and enterprise versions of Windows 10 or Windows 11.

Convert Surface Hub to run Pro or Enterprise desktop

You can change the OS on Surface Hub 2S by migrating to Windows 10 or Windows 11 Pro/Enterprise. To learn more, see the following resources:

- Announcing the availability of Windows 10 Pro and Enterprise on Surface Hub 2.
- Migrate to Windows 10 or Windows 11 Pro or Enterprise on Surface Hub 2

User interface

Shell (OS user interface)

The Surface Hub's shell is designed from the ground up to be large screen and touch optimized. It doesn't use the same shell as Windows 10 or Windows 11 Enterprise.

Potential impact on organization policies:

- Settings related to controls in the Windows 10 or Windows 11 Enterprise shell don't apply for Surface Hub.

Lock screen and screensaver

Surface Hub doesn't have a lock screen or a screen saver, but it has a similar feature called the welcome screen. The welcome screen shows scheduled meetings from the

device account's calendar, and easy entry points to the Surface Hub's top apps - Skype for Business, Whiteboard, and Connect.

Potential impact on organization policies:

- Settings for lock screen, screen timeout, and screen saver don't apply for Surface Hub.

User sign-in

Unlike Windows PCs, anyone can walk up and use a Surface Hub without requiring a user to sign in. To enable this communal functionality, Surface Hub doesn't support Windows sign-in the same way that Windows 10 or Windows 11 Enterprise does (for example, signing in a user to the OS and using those credentials throughout the OS). Instead, there's always a local, auto signed-in, low-privilege user signed in to the Surface Hub. It doesn't support signing in any more users, including admin users (for example, when an admin signs in, they aren't signed in to the OS).

Users can sign in to a Surface Hub, but they won't be signed in to the OS. For example, when a user signs in to Apps or My Meetings and Files, the user is signed in only to the apps or services, not to the OS. As a result, the signed-in user is able to retrieve their cloud files and personal meetings stored in the cloud, and these credentials are discarded when **End session** is activated. The Meetings and Files sign-in process doesn't support EWSAllowList or EWSBlockList policies.

Potential impact on organization policies:

- Generally, Surface Hub uses lockdown features rather than user access control to enforce security. Policies related to password requirements, interactive sign in, user accounts, and access control don't apply for Surface Hub.

Saving and browsing files

Users have access to a limited set of directories on the Surface Hub:

- Music
- Videos
- Documents
- Pictures
- Downloads

Files saved locally in these directories are deleted when users press **End session**. To save content created during a meeting, users should save files to a USB drive or to OneDrive.

Potential impact on organization policies: - Policies related to access permissions and ownership of files and folders don't apply for Surface Hub. Users can't browse and save files to system directories and network folders.

Applications

Default applications

With few exceptions, the default Universal Windows Platform (UWP) apps on Surface Hub are also available on Windows 10 or Windows 11 PCs.

UWP apps pre-installed on Surface Hub:

- Alarms & Clock
- Calculator
- Connect
- Excel Mobile
- Feedback Hub
- File Explorer
- Get Started
- Maps
- Microsoft Edge
- Microsoft Power BI
- Microsoft Teams
- Microsoft Whiteboard
- OneDrive
- Photos
- PowerPoint Mobile
- Settings
- Store
- Tips
- Word Mobile

Potential impact on organization policies:

- Use guidelines for Windows 10 or Windows 11 Enterprise to determine the features and network requirements for default apps on the Surface Hub.

Installing apps, drivers, and services

To help preserve the appliance-like nature of the device, Surface Hub only supports installing Universal Windows Platform (UWP) apps, and doesn't support installing classic Win32 apps, services and drivers. Furthermore, only admins have access to install UWP apps.

Potential impact on organization policies:

- Employees can only use the apps that have been installed by admins, helping mitigate against unintended use. Surface Hub doesn't support installing Win32 agents required by most traditional PC management and monitoring tools.

Security and lockdown

For Surface Hub to be used in communal spaces, such as meeting rooms, its custom OS implements many of the security and lockdown features available in Windows 10 or Windows 11. To learn more, see Surface Hub Security Overview

Surface Hub implements these Windows security features:

- Secure Boot
- Windows Defender Application Control and virtualization-based protection of code integrity
- Application restriction policies using AppLocker
- BitLocker Drive Encryption
- Trusted Platform Module (TPM)
- Microsoft Defender Antivirus in Windows
- User Account Control (UAC) for access to the Settings app

These Surface Hub features provide more security:

- Custom UEFI firmware
- Custom shell and Start menu limits device to meeting functions
- Custom File Explorer only grants access to files and folders under My Documents
- Custom Settings app only allows admins to modify device settings
- Downloading advanced Plug and Play drivers is disabled

Potential impact on organization policies:

- Consider these features when performing your security assessment for Surface Hub.

Management

Device settings

Device settings can be configured through the Settings app. The Settings app is customized for Surface Hub, but also contains many familiar settings from Windows 10 or Windows 11 Desktop. A User Accounts Control (UAC) prompt appears when opening up the Settings app to verify the admin's credentials, but this doesn't sign in the admin.

Potential impact on organization policies:

- Employees can use the Surface Hub for meetings, but can't modify any device settings. In addition to lockdown features, this ensures that employees only use the device for meeting functions.

Administrative features

The administrative features in Windows 10 or Windows 11 Enterprise, such as the Microsoft Management Console, Run, Command Prompt, PowerShell, Registry editor, and Task manager aren't supported on Surface Hub. The Settings app contains all of the administrative features locally available on Surface Hub.

Event viewer

Windows 10 Team 2020 Update 2 adds support for the Windows Event Viewer, which is identical to the Event Viewer installed on Windows 10 Pro or Windows 10 Enterprise.

To open Event viewer:

1. Sign in to **Settings** app with admin credentials.
2. Select **Update & Security** > **Logs** and under Event Viewer, select **Open**.

To learn more, see Windows Event Viewer.

Remote management and monitoring

Surface Hub supports remote management through mobile device management (MDM) solutions such as Microsoft Intune and monitoring through Azure Monitor.

Potential impact on organization policies:

- Surface Hub doesn't support installing Win32 agents required by most traditional PC management and monitoring tools, such as System Center Operations Manager.

Group Policy

Surface Hub doesn't support Windows Group Policy, including auditing. Instead, use MDM to apply policies to your Surface Hub. For more information about MDM, see Manage settings with an MDM provider.

Potential impact on organization policies:

- Use MDM to manage Surface Hub rather than group policy.

Remote assistance

Surface Hub doesn't support remote assistance.

Potential impact on organization policies:

- Policies related to remote assistance don't apply for Surface Hub.

Network

Domain join and Azure Active Directory (Azure AD) join

Surface Hub uses domain join and Azure AD join primarily to provide a directory-backed admin group. Hybrid join isn't supported. Users can't sign in with a domain account. For more information, see Admin group management.

Potential impact on organization policies:

- Group policy settings aren't applied when a Surface Hub is joined to your domain. Policy settings related to domain membership don't apply to Surface Hub.

Accessing domain resources

Users can sign in to Microsoft Edge to access intranet sites and online resources (such as Microsoft 365). If your Surface Hub is configured with a device account, the system uses it to access Exchange, Microsoft Teams Rooms, or Skype for Business. However, Surface Hub doesn't support accessing domain resources such as file shares and printers.

Potential impact on organization policies:

- Policies related to accessing domain objects don't apply for Surface Hub.

Diagnostic data

The Surface Hub OS uses the Windows Connected User Experience to gather and transmit diagnostic data. For more information, see Configure Windows diagnostic data in your organization.

Potential impact on organization policies:

- Configure diagnostic data levels for Surface Hub in the same way as you do for Windows 10 or Windows 11 Enterprise.

Surface Hub 2S camera lens orientation

Article • 05/11/2023

Surface Hub 2S comes with an external camera accessory that can be mounted to any of the four (4) USB-C ports on the bezel of the display. It is recommended to place the camera on the top center of the display to provide the widest field of view for remote meeting participants.

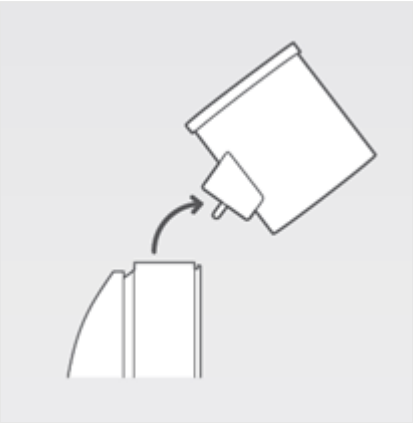
Applies to: Surface Hub 2S - 50 inch
Original KB number: 4509729

Summary

By default, the camera lens orientation is configured for top mounting but if a customer chooses to side mount, the camera lens orientation will need to be manually rotated.

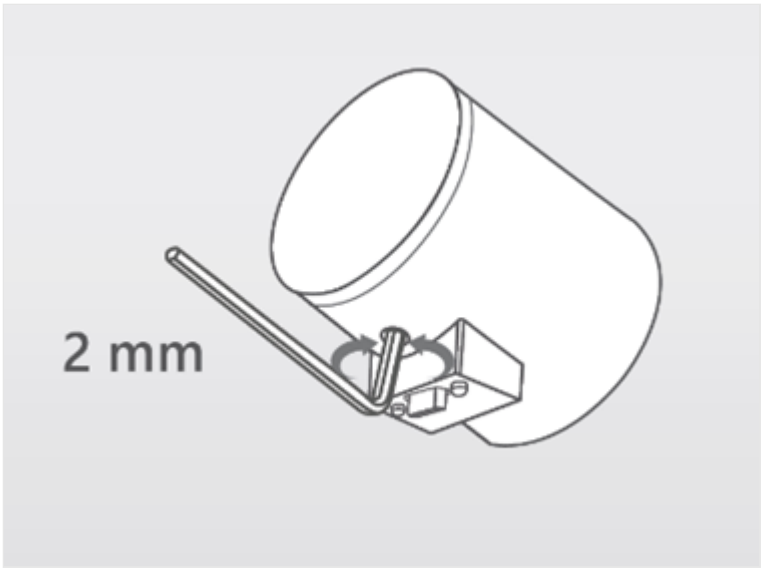
This rotation can be achieved by the following steps:

1. Power off the Surface Hub 2S, then unmount the Camera from the display by gently tilting the camera body towards the front of the display until it detaches.

2. Locate the camera orientation driver pin on the bottom of the camera body. Use a 2mm hex key to rotate the driver pin one full turn, until you feel the driver pin stop.

   > **Note**
   >
   > You should hear the camera lens rotate when it flips to the new orientation. Be careful not to force or over rotate the lens.



3. Return the camera to the top or side of the device, depending on preference, and power the device up. Verify the correct orientation of the camera lens by initiating a Teams or Skype for Business call, or by using the Surface Hub Hardware Diagnostic Application.

Start and finish a meeting on Surface Hub

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

Surface Hub is a collaboration device designed to be used in meeting spaces by different groups of people. This page explains how to start and finish a meeting plus how to save or share your work during collaboration.

Meet with others on Surface Hub 2S

Have an ad-hoc meeting

If no scheduled meetings are listed on the welcome screen, the Surface Hub is free to use—sign in and start working.

How you meet is up to you—you can open Microsoft Whiteboard and start drawing out your ideas, open up your recent files to see them on the big screen, get real-time feedback from your team, and start a call with Teams or Skype. Get creative and work however, works best for that moment—it's up to you.

Schedule a meeting

It's easy to schedule a meeting on a Surface Hub—invite it to the meeting like you would a person. Include the Surface Hub on the invite list of your meeting—you'll be able to see its availability just like you can the other people you're inviting.

If you need to know the name of the Surface Hub you want, select **Call** on the welcome screen and then look for the email address of the Surface Hub listed under **Organizer**. That's the email address you should invite to your meeting.

Start a scheduled meeting

If you've scheduled a meeting on a Surface Hub, you should see your name listed on the welcome screen along with the time of the meeting. To start your meeting, select **Join**, and you'll immediately enter the meeting. If your meeting includes Teams or Skype, the call will also begin.

Add someone to a call on Surface Hub

Add someone to a call using Teams:

1. Select **Show participants**.
2. Enter the name or email address of the person you want to add in the box that says **Invite someone**.
3. Or, dial the phone number of the person you want to add.

Add someone to a call on a Surface Hub using Skype:

1. Select **People** at the bottom of the Skype pane, then **Add.**
2. Enter the name or email address of the person you want to add or dial their number.

Share the Surface Hub screen during a call

Share the screen using Teams:

1. Select **Share**. You'll see a yellow outline around the content you're presenting on the screen.
2. To stop sharing without hanging up, select **Stop sharing**.

Share the screen using Skype:

1. Select **Present screen**.
2. To stop presenting without hanging up, select **Stop presenting**.

Finish a Surface Hub meeting with End session

At the end of a meeting, users can tap **End session** to clean up any sensitive data and prepare the device for the next meeting. Surface Hub will clean up, or reset, the following states:

- Applications
- Operating system
- User interface

This section explains what **End session** resets for each of these states.

Applications

When you start apps on Surface Hub, they are stored in memory and data is stored at the application level. Data is available to all users during that session (or meeting) until data is removed or overwritten. When **End session** is selected, Surface Hub application

state is cleared out by closing applications, deleting browser history, resetting applications, and removing Skype logs.

Close applications

Surface Hub closes all visible windows, including Win32 and Universal Windows Platform (UWP) applications. The application close stage uses the multitasking view to query the visible windows. Win32 windows that do not close within a certain timeframe are closed using **TerminateProcess**.

Delete browser history

Surface Hub uses Delete Browser History (DBH) in Edge to clear Edge history and cached data. This is similar to how a user can manually clear out their browser history, but **End session** also ensures that application states are cleared and data is removed before the next session, or meeting, starts.

Reset applications

End session resets the state of each application installed on the Surface Hub. Resetting an application clears all background tasks, application data, notifications, and user consent dialogs. Applications are returned to their first-run state for the next people that use Surface Hub.

Remove Skype logs

Skype does not store personally-identifiable information on Surface Hub. Information is stored in the Skype service to meet existing Skype for Business guidance. Local Skype logging information is the only data removed when **End session** is selected. This includes Unified Communications Client Platform (UCCP) logs and media logs.

Operating System

The operating system hosts a variety of information about the state of the sessions that needs to be cleared after each Surface Hub meeting.

File System

Meeting attendees have access to a limited set of directories on the Surface Hub. When **End session** is selected, Surface Hub clears these directories:

- Music
- Videos
- Documents
- Pictures
- Downloads

Surface Hub also clears these directories, since many applications often write to them:

- Desktop
- Favorites
- Recent
- Public Documents
- Public Music
- Public Videos
- Public Downloads

Credentials

User credentials stored in **TokenBroker**, **PasswordVault**, or **Credential Manager** are cleared when you tap **End session**.

User interface

User interface (UI) settings are returned to their default values when **End session** is selected.

UI items

- Reset Quick Actions to default state
- Clear Toast notifications
- Reset volume levels
- Reset sidebar width
- Reset tablet mode layout
- Sign user out of Microsoft 365 meetings and files

Accessibility

Accessibility features and apps are returned to default settings when **End session** is selected.

- Filter keys

- High contrast
- Sticky keys
- Toggle keys
- Mouse keys
- Magnifier
- Narrator

Clipboard

The clipboard is cleared to remove data that was copied to the clipboard during the session.

Frequently asked questions

What happens if I forget to tap End session at the end of a meeting, and someone else uses the Surface Hub later?

- Surface Hub only cleans up meeting content when users tap **End session**. If you leave the meeting without tapping **End session**, the device will return to the welcome screen after some time. From the welcome screen, users can resume the previous session or start a new one. You can also disable the ability to resume a session if **End session** is not pressed.

Are documents recoverable?

- Removing files from the hard drive when **End session** is selected is just like any other file deletion from a hard disk drive. Third-party software might be able to recover data from the hard disk drive, but file recovery is not a supported feature on Surface Hub. To prevent data loss, always save the data you need before leaving a meeting.

Do the clean-up actions from End session comply with the US Department of Defense clearing and sanitizing standard: DoD 5220.22-M?

- No. Currently, the clean-up actions from **End session** do not comply with this standard.

Save or share your work on Surface Hub

The easiest way to save your work is to sign in to Surface Hub. That way, you'll also be automatically signed in to Microsoft 365, and your work will save automatically to

OneDrive or SharePoint—whatever you have set up already with your organization's Microsoft 365 subscription.

Autosave means you don't have to worry about losing work after collaborating on Surface Hub. All your notes, revisions, changes, and additions will stay synced in your file.

Set up and use Microsoft Whiteboard

Article • 02/16/2023

The Microsoft Whiteboard app includes the capability for Surface Hubs and other devices with the Microsoft Whiteboard app installed to collaborate in real time on the same board.

Prerequisites

To use whiteboard collaboration, complete the following actions:

- Add Whiteboard.ms, whiteboard.microsoft.com, and wbd.ms to your list of allowed sites.
- Open port: **HTTPS: 443** (normally configured when you first run Surface Hub.)
- Ensure that Whiteboard is enabled for your organization. For more information, see Manage access to Whiteboard.

Microsoft 365 requirements

- Whiteboard collaboration is only supported in the Microsoft 365 commercial environment and requires Microsoft 365 with cloud-based Azure Active Directory (Azure AD).
- You can only run collaborative sessions among users belonging to the same Microsoft 365 tenant.
- Microsoft 365 Germany or Microsoft 365 operated by 21Vianet don't support whiteboard collaboration.

Collaborating with whiteboards

To start a collaboration session:

1. In the Whiteboard app, tap the **Sign in** button.
2. Sign in with your organization ID.
3. Tap the **Invite** button next to your name at the top of the app.
4. Write or type the names of the colleagues you wish to collaborate with.

On the other device, such as a Surface Hub, when you're signed in, the shared board will now appear in the board gallery.

User tips

- Sign in to access your whiteboards. As you work, changes are saved automatically.
- Name your whiteboards to help organize your content and find it quickly. Select the ... to open the menu. Select the **Options** gear icon to access more tools and features of the Whiteboard.
- Use **Ink to shape** to turn drawing into actual shapes like circles, squares, and triangles.
- Use **Ink to table** to turn a drawn grid into a table with rows and columns.
- You can also change the background color and design from solid to grid or dots. Pick the background, then choose the color from the wheel around it.
- You can export a copy of the Whiteboard collaboration for yourself through the Share charm and leave the board for others to continue working.

For more information, see Use Microsoft Whiteboard on a Surface Hub.

> **Tip**
>
> If you are using Whiteboard and cannot sign in, you can collaborate by joining a Teams or Skype for Business meeting, and then sharing your screen. After you're done, tap **Settings** > **Export to email** or save a copy of the board. If you choose to export to SVG, it exports vector graphics and provides higher resolution than PNG and can be opened in a web browser.

New features in Whiteboard

The Microsoft Whiteboard app, updated for Surface Hub on July 1, 2019 includes a host of new features including:

- **Automatic Saving** - Boards are saved to the cloud automatically when you sign in, and can be found in the board gallery. There's no local folder name or directory.
- **Extended collaboration across devices** - You can collaborate using new apps for Windows 10 or Windows 11 PC and iOS, and a web version for other devices.
- **Richer canvas** - In addition to ink and images, Whiteboard now includes sticky notes, text and GIFs, with more objects coming soon.
- **Intelligence** – In addition to ink to shape and table, Whiteboard now includes ink beautification to improve handwriting and ink grab to convert images to ink.
- **More color and background options** - Whiteboard now includes more pen colors and thickness options along with other background colors and designs.

- **Teams Integration** – You can automatically launch Whiteboard from a Teams meeting and share with participants.

Related articles

- Support documentation for Microsoft Whiteboard
- Use Microsoft Whiteboard on a Surface Hub

Adjust accessibility settings on Surface Hub

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

Microsoft Surface Hub has a variety of accessibility (Ease of Access) options. New in Windows 10 Team 2020 Update 2:

- Users can adjust Ease of Access settings for the duration of a Surface Hub session. When the session ends, Ease of Access settings revert to their default state.
- Users can close apps on Surface Hub by selecting the close button, in the top right corner of the app, just like they do in other versions of Windows 10. This removes the need to close apps by dragging them to the bottom of the Surface Hub display.

Default Ease of Acess settings

Admins can manage Ease of Access settings so they remain in effect across all user sessions. With the exception of Mouse settings, users can adjust the default behavior, as shown in the following table.

Ease of Access feature	**Default settings**	**Availability**
Magnifier	Off	Admins & users
High contrast	No theme selected	Admins & users
Closed captions	Defaults selected for Font and Background and window	Admins & users
Keyboard	**On-screen Keyboard**, **Sticky Keys**, **Toggle Keys**, and **Filter Keys** are all off.	Admins & users
Mouse	Defaults selected for **Pointer size**, **Pointer color** and **Mouse keys**.	Admins only
Other options	Defaults selected for **Visual options** and **Touch feedback**.	Admins & users

Ease of access settings

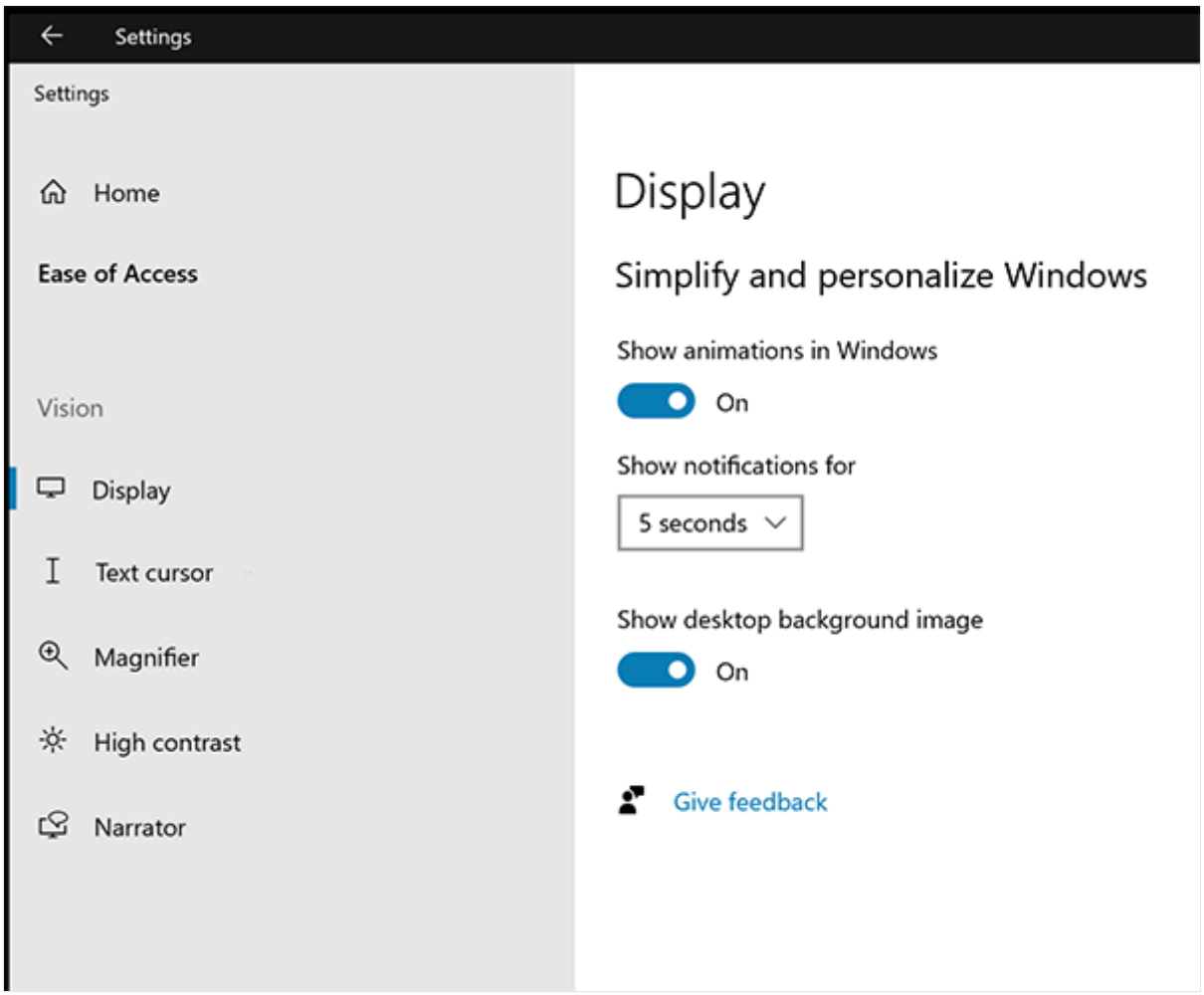
During a Surface Hub session, users can adjust Ease of Access settings.

- Select **Start** > **Settings** > **Ease of Access**.

Display

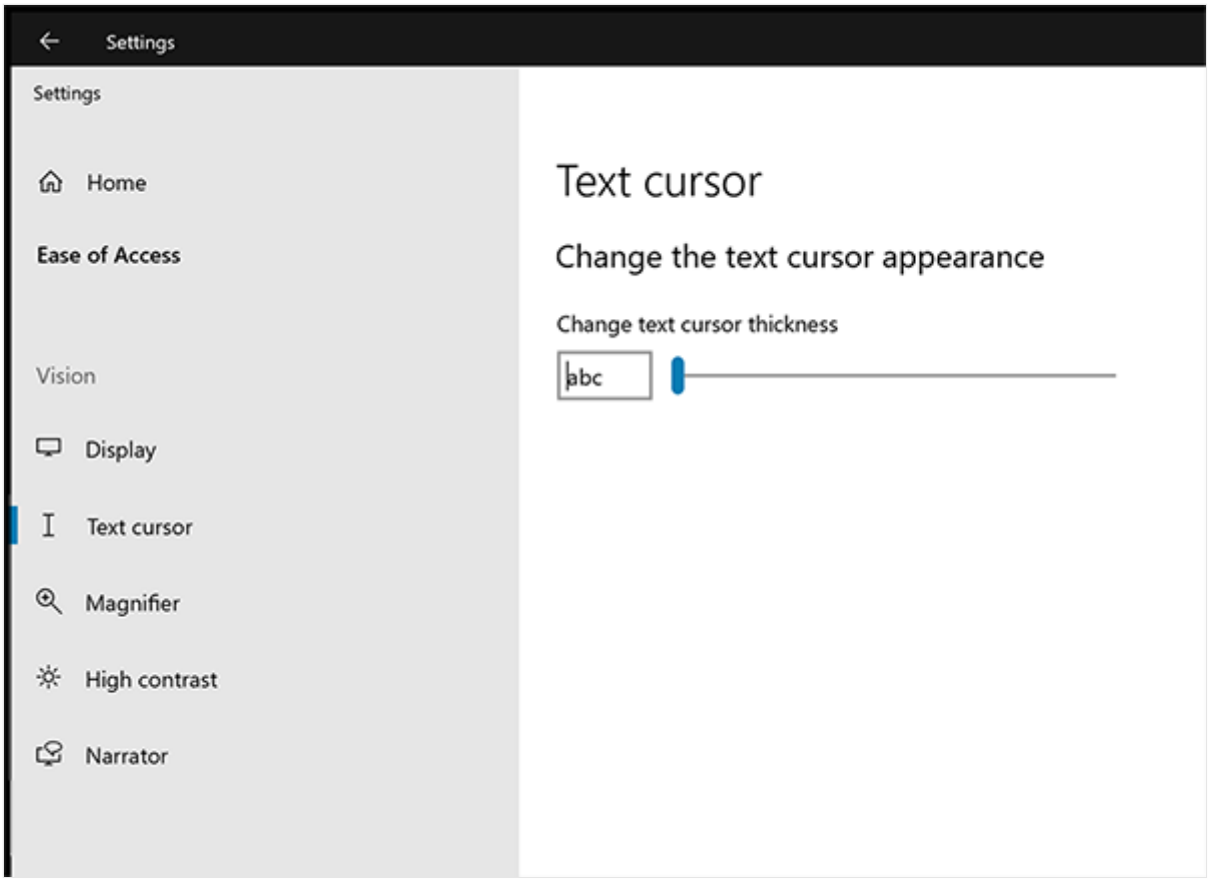
- Simplify and personalize Surface Hub.
- Minimize visual distractions by turning off animations.

By default, Surface Hub notifications disappear five seconds after they appear. If you want more time to read them, you can increase how long they're displayed.



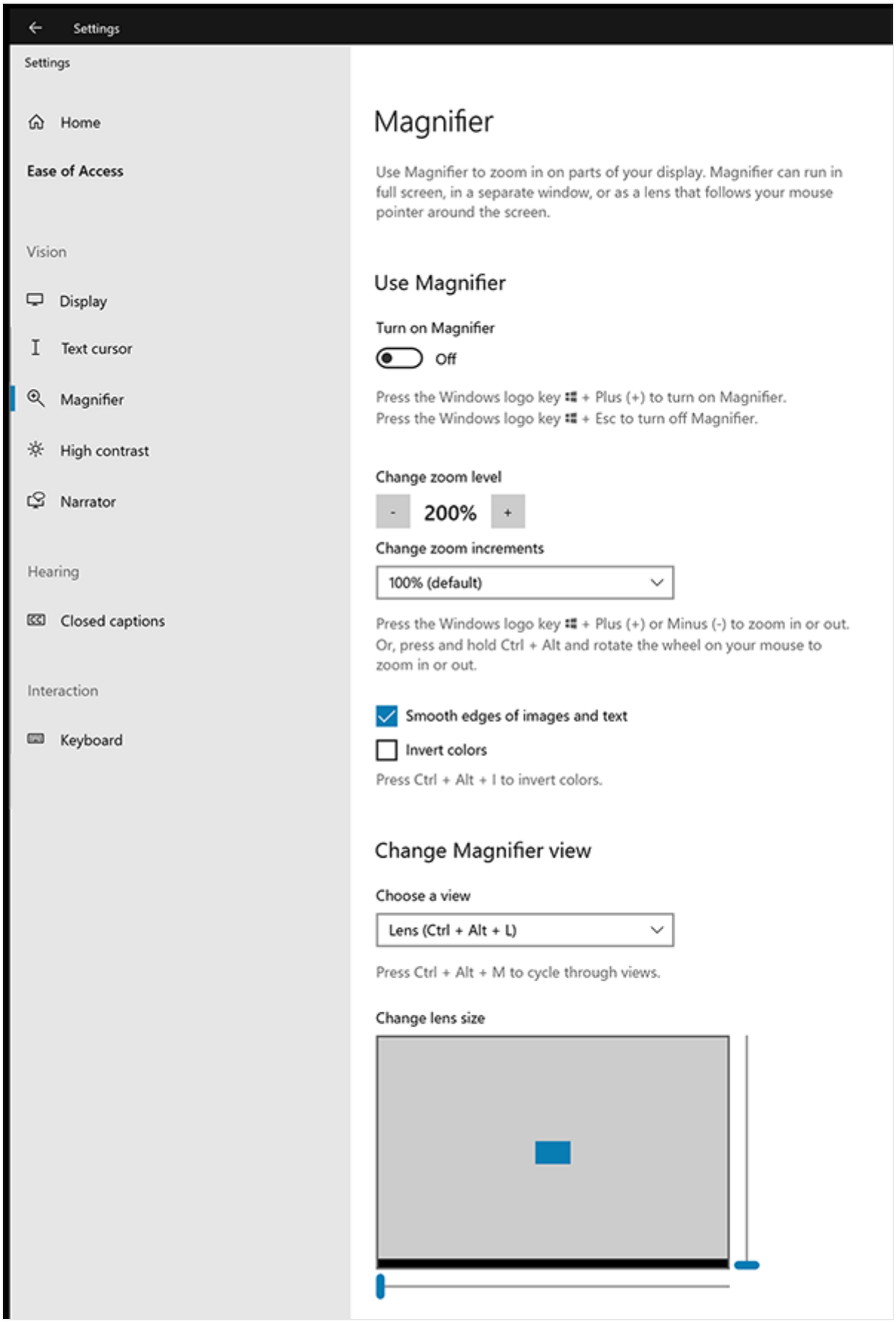
Text cursor

Change the text cursor to make it easier to see.



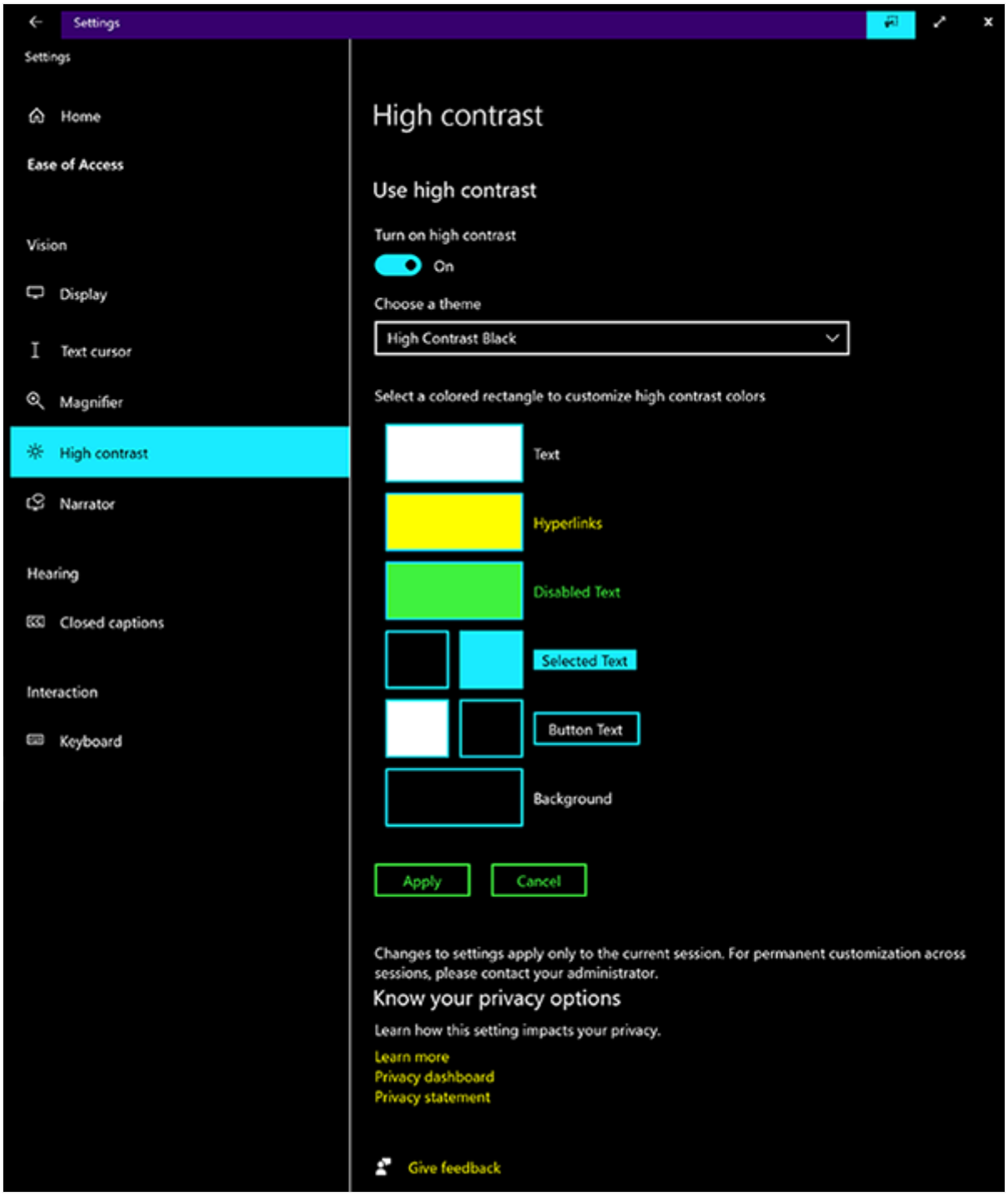
Magnifier

Enlarge all or part of your screen.



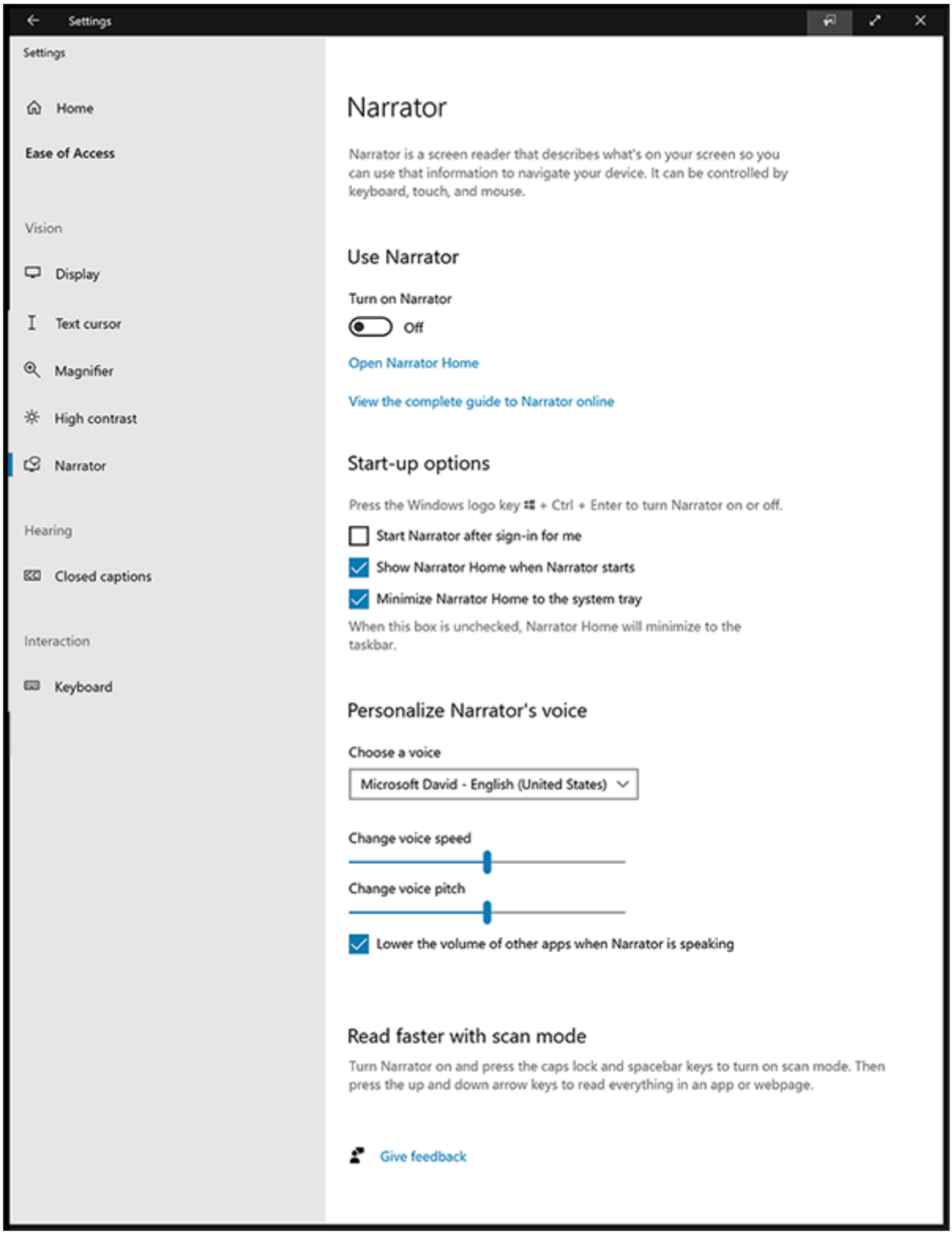
High contrast

Pick a high-contrast theme to suit your needs.



Narrator

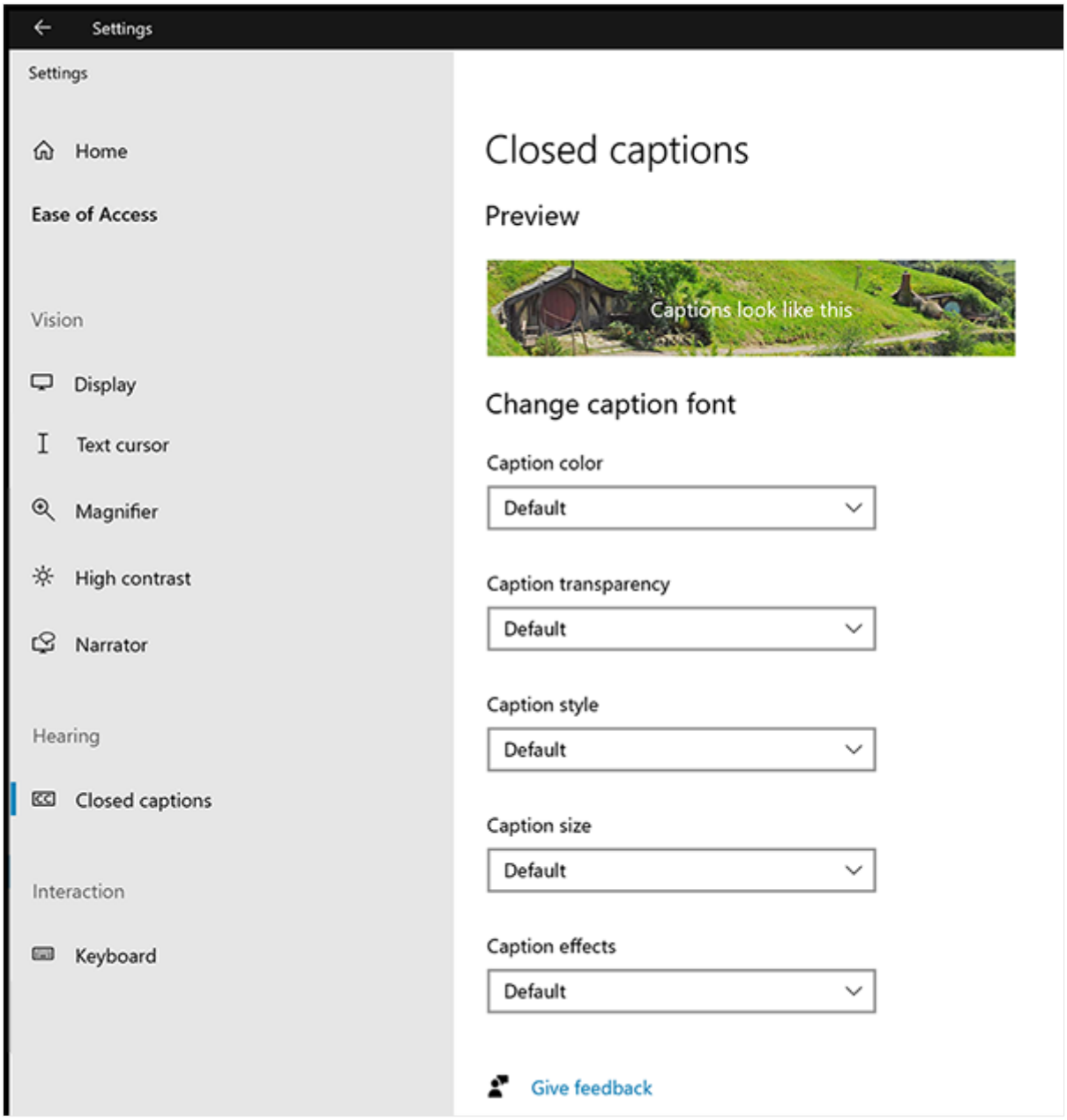
Turn on Narrator to describe Windows and apps. Control Surface Hub using a keyboard, controller, or gestures.



Closed captions

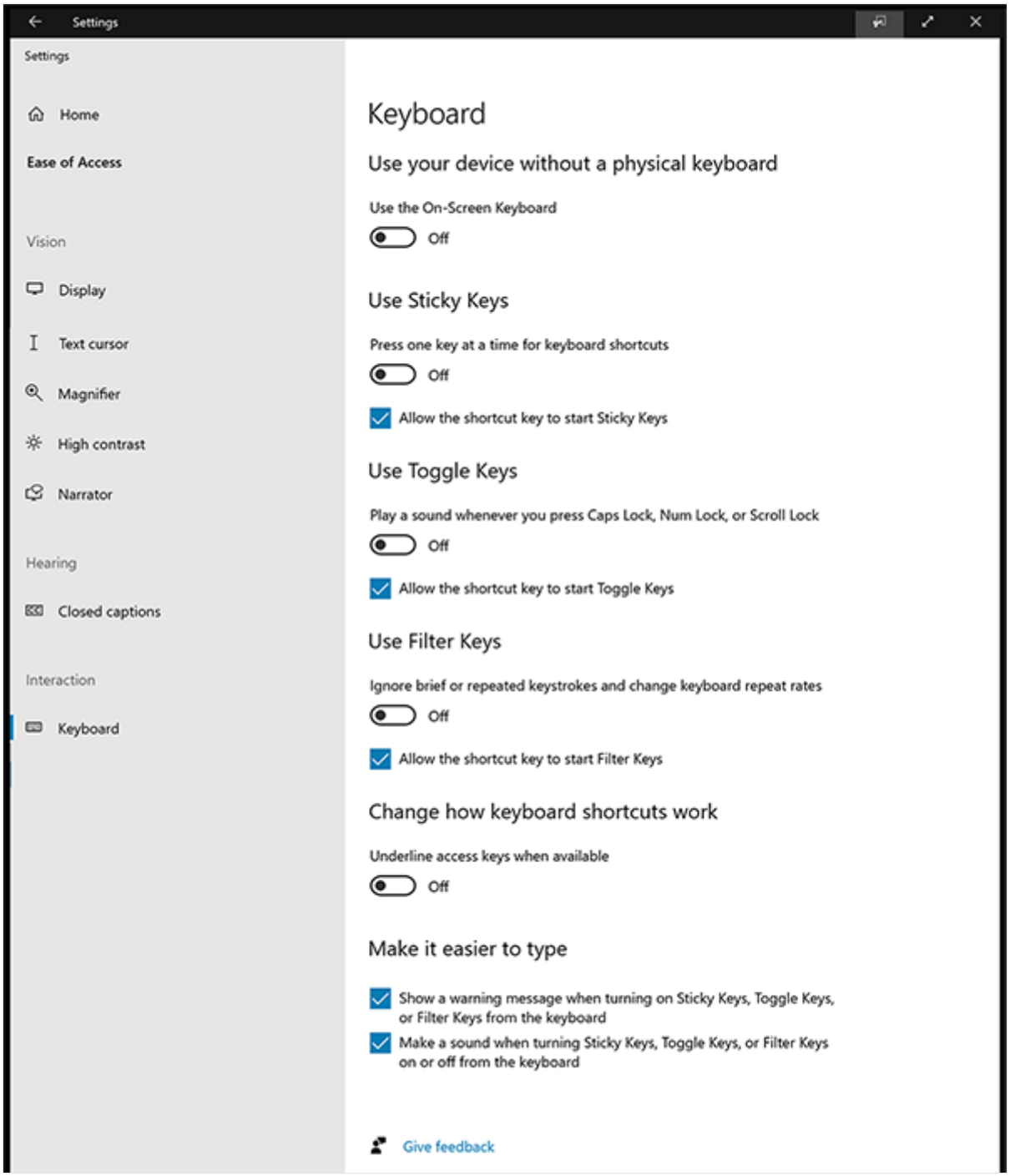
Customize things like the color, transparency and size of closed captions.

- Color: White, black, red, green, blue, yellow, magenta, and cyan
- Transparency: opaque, translucent, semitransparent, and transparent
- Size: 50%, 100%, 150%, and 200%



Keyboard

Change how you interact with Surface Hub with options like an on-screen keyboard, toggle keys, sticky keys, and more.



Keyboard shortcuts

Keyboard shortcuts	Action	Use when you want to:
Start key + ENTER	Turns Narrator on or off	Have Narrator read aloud the text highlighted on the screen
Start key + =	Increases magnification Opens the magnifier	Enlarge everything on the screen or everything in the magnifier lens (You can also select the + on the magnifier toolbar.)

Keyboard shortcuts	Action	Use when you want to:
Start key + -	Reduces magnification	Shrink everything on the screen. (You can also select the - on the magnifier toolbar.)
Right shift for eight seconds	Turns Filter Keys on or off.	Ignore or slow down brief or repeated keystrokes and adjust keyboard repeat rates.
Shift five times	Turns Sticky Keys on or off.	Press one key at a time for keyboard shortcuts.

Change display language on Surface Hub

Article • 03/21/2023 • Applies to: Surface Hub, Surface Hub 2S

Surface Hub now allows end users to change the display language and preferred language, just like in other versions of Windows 10.

Once a Surface Hub admin installs extra languages, users can change the display language by selecting a new one from the available installed languages.

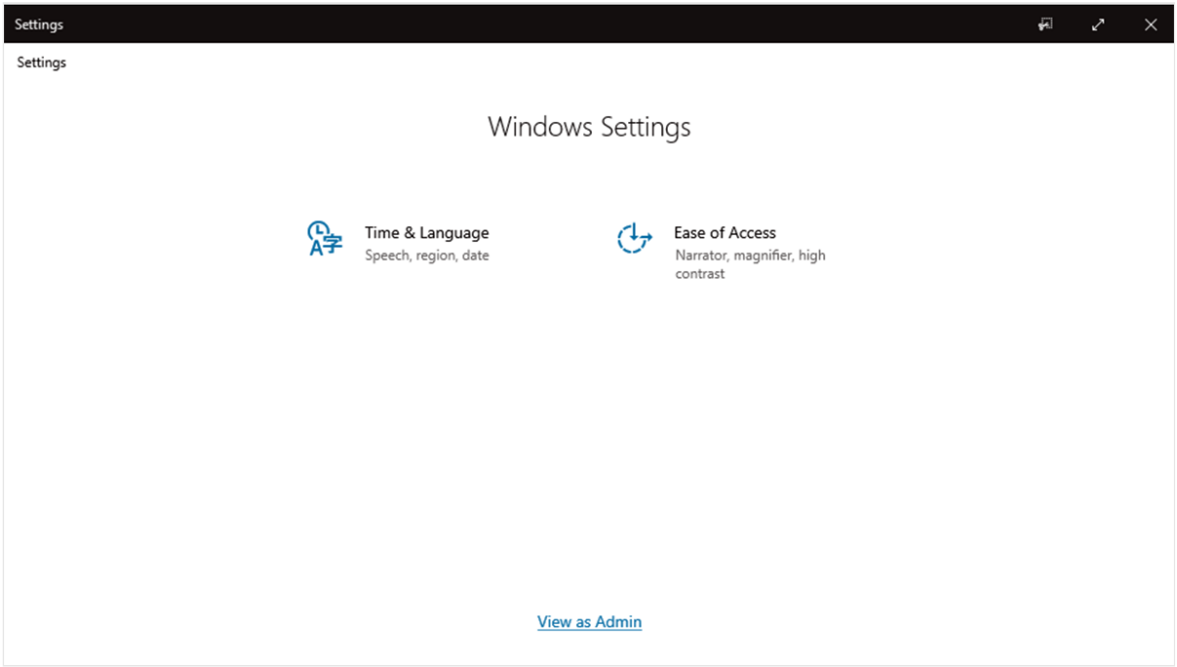
> **Note**
>
> Only Surface Hub admins can install additional languages for availability to end users. First, ensure that your Surface Hub has **KB5023773** (or a subsequent Windows update) installed. To learn more about the latest Windows 10 Team updates, refer to **Surface Hub update history**.

End user language option

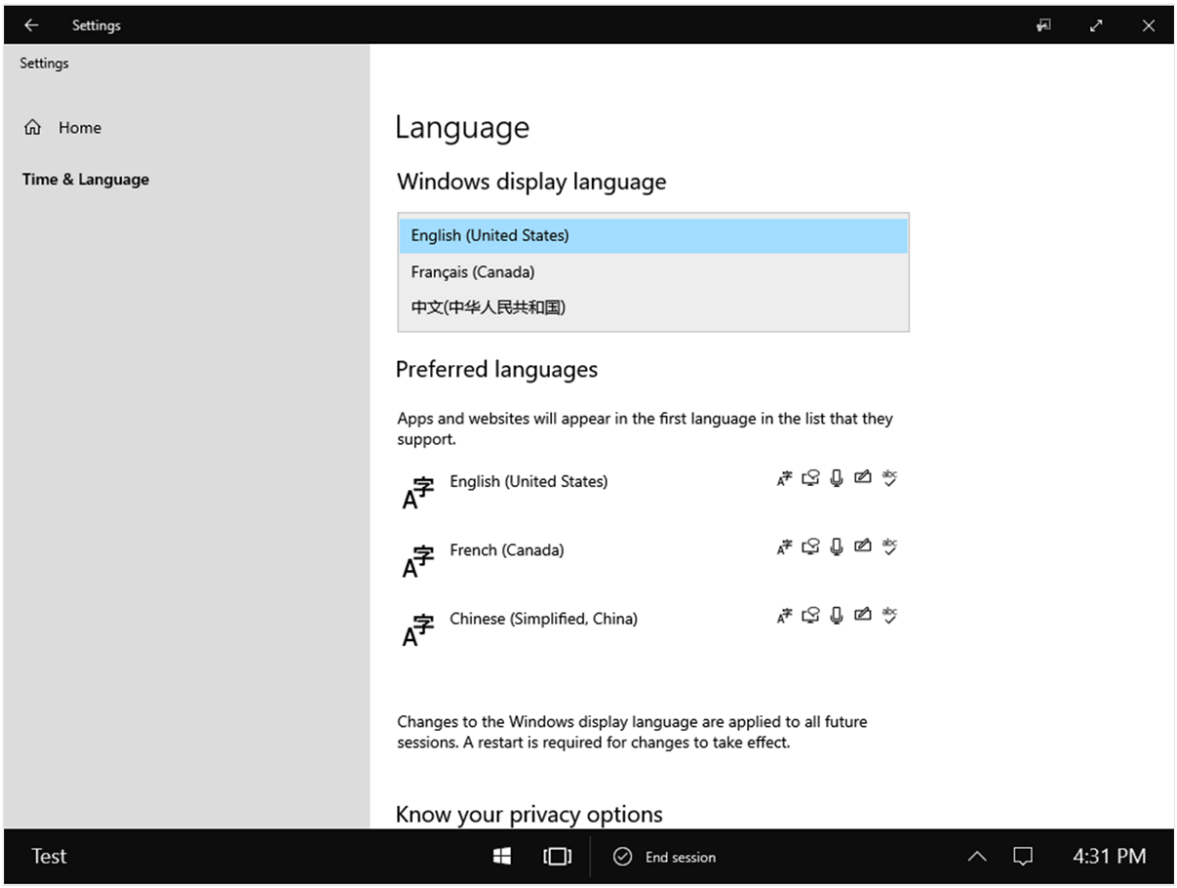
Users can change the display language on Surface Hub via a similar process used on desktop versions of Windows 10.

Change the Display language

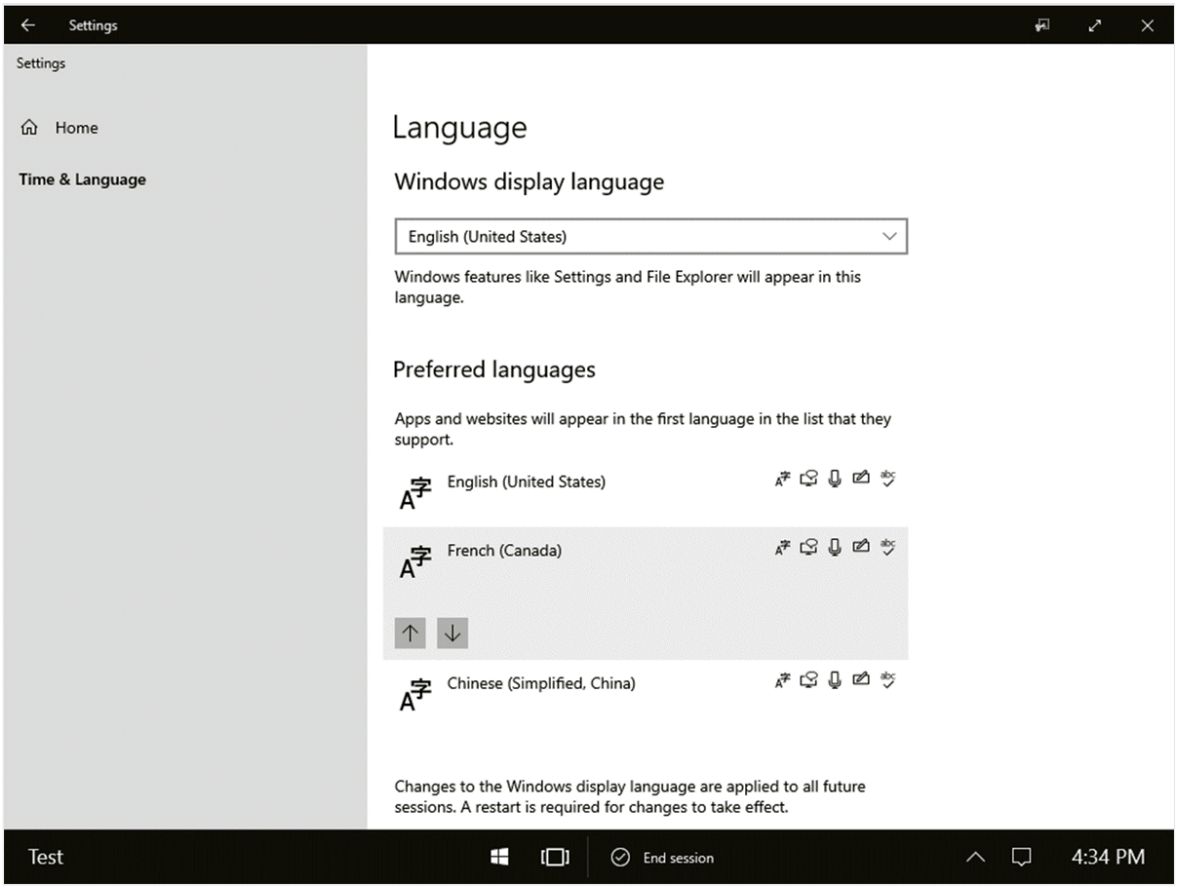
1. Select **Start** > **Settings** > **Time & Language**.



2. Choose from the available languages as installed by your Surface Hub admin.



3. Optional: For best results, also move the new language to the top of the **Preferred languages** list.



4. Restart Surface Hub.

> **Note**
>
> The new language setting remains in effect for all future sessions unless changed by another user or an admin. Unlike other user-modified settings, the chosen language is not removed when a user selects **End session.**

Admin-only settings

To enable users to change the display language on Surface Hub, admins must first install the desired languages and related options, such as keyboard settings.

Modify language settings

1. Select **Start -> Settings -> Time & Language > View as Admin** and sign in with your admin credentials.
2. Install languages based on the users' geography, diversity, and preferences to enable an inclusive and seamless interaction with the device in the collaboration space.
3. Use the same procedure described in Manage the input and display language settings in Windows.

> **Note**
>
> When end users change the display language, some screens that display admin-only info are not switched to the newly selected language.

> **Tip**
>
> Admins can also install a keyboard layout for another language without switching the user interface. This may be useful for users who collaborate in English and communicate with colleagues in another language.

Learn more

- Manage the input and display language settings in Windows
- Install Windows 10 Team 2022 Update
- Surface Hub update history
- Adjust accessibility settings

Adjust Surface Hub 2S brightness, volume, and input

Article • 01/03/2023

Surface Hub 2S provides an on-screen display for volume, brightness, and input control. The Source button functions as a toggle key to switch between the volume, brightness, and input control menus.

To show the on-screen display

- Press and hold the **Source** button for 4 seconds.

When the on-screen display is visible, use one or more buttons to reach desired settings.

To adjust volume

- Use the **Volume up/down** button to increase or decrease volume.

To adjust brightness

1. Press the **Source** button again to switch to the brightness menu.
2. Use the **Volume up/down** button to increase or decrease brightness.

To adjust input

1. Press the **Source** button twice to switch to the Source menu.
2. Use the **Volume up/down** button to switch between PC, HDMI, and USB-C inputs.

Using the Surface app on Surface Hub 2S

Article • 05/11/2023

This article describes how to use the Surface app on Surface Hub 2S.

Applies to: Surface Hub 2S - 50 inch
Original KB number: 4510098

> **Note**
>
> Some products might not be available in your country or region.

You can use the Surface App on Surface Hub 2S to adjust your Surface Hub 2 Pen pressure, see the battery health of connected bluetooth accessories, and see info about your device like its name and serial number.

To open the Surface App on your Surface Hub 2S, select **Start** > **All apps** > **Surface**.

- Select **Audio**  to adjust the audio settings on your Surface Hub 2S.
- Select **Battery level** to see the battery health of your connected bluetooth devices. If you need to connect a Bluetooth device to your Surface Hub, contact your organization's support person. Bluetooth devices are paired through Settings.
- Select **Pen**  to adjust your pen pressure, adjust inking thickness, and see pen responsiveness and sensitivity graphs. Some additional options can be found when you select **Advanced**.
- Select **Your Surface**  to see your Surface Hub's device name, serial number, model, as well as UEFI and driver versions.
- Select **Safety, regulatory, and warranty information**  to see safety, health, and warranty info.

Manage Surface Hub

Article • 02/16/2023

After initial setup of Surface Hub, you can modify device settings and configuration:

- **Local management** - Every Surface Hub can be configured locally using the **Settings** app on the device. To prevent unauthorized users from changing settings, the Settings app requires admin credentials to open the app. For more information, see Local management for Surface Hub settings.
- **Remote management** - Surface Hub allow IT admins to manage settings and policies using a mobile device management (MDM) provider, such as Microsoft Intune, Microsoft Endpoint Configuration Manager, and other third-party providers. Additionally, admins can monitor Surface Hubs using Azure Monitor. For more information, see Manage settings with an MDM provider, and Monitor Surface Hubs with Azure Monitor to track their health.

> **Tip**
>
> These management methods are not mutually exclusive. Devices can be both locally and remotely managed if you choose. However, MDM policies and settings will overwrite local changes when the Surface Hub syncs with the management server.

In this section

Learn about managing and updating Surface Hub.

Topic	Description
Remote Surface Hub management	Topics related to managing your Surface Hub remotely. Include install apps, managing settings with MDM and monitoring with Operations Management Suite.
Manage Surface Hub settings	Topics related to managing Surface Hub settings: accessibility, device account, device reset, fully qualified domain name, Windows Update settings, and wireless network
Install apps on your Surface Hub	Admins can install apps can from either the Microsoft Store or the Microsoft Store for Business.
Configure Surface Hub Start menu	Use MDM to customize the Start menu for Surface Hub.

Topic	Description
Set up and use Microsoft Whiteboard	Microsoft Whiteboard's latest update includes the capability for two Surface Hubs to collaborate in real time on the same board.
End a meeting with End session	At the end of a meeting, users can tap **End session** to clean up any sensitive data and prepare the device for the next meeting.
Sign in to Surface Hub with Microsoft Authenticator	You can sign in to a Surface Hub without a password using the Microsoft Authenticator app, available on Android and iOS.
Save your BitLocker key	Every Surface Hub is automatically set up with BitLocker drive encryption software. Microsoft strongly recommends that you make sure you back up your BitLocker recovery keys.
Connect other devices and display with Surface Hub	You can connect other device to your Surface Hub to display content.
Miracast on existing wireless network or LAN	You can use Miracast on your wireless network or LAN to connect to Surface Hub.
Enable 802.1x wired authentication	802.1x Wired Authentication MDM policies have been enabled on Surface Hub devices.
Using a room control system	Room control systems can be used with your Microsoft Surface Hub.
Using the Surface Hub Recovery Tool	Use the Surface Hub Recovery Tool to re-image the Surface Hub SSD.
Surface Hub SSD replacement	Learn how to remove and replace the solid state drive in your Surface Hub.

Related topics

- View reports and dashboards in presentation mode on Surface Hub and Windows 10 devices

Manage Surface Hub with an MDM provider

Article • 04/19/2023 • Applies to: Surface Hub 2S, Surface Hub

Surface Hub allows IT administrators to manage settings and policies using a mobile device management (MDM) provider such as Microsoft Intune. Surface Hub has a built-in management component to communicate with the management server. There is no need to install additional clients on the device.

To enroll, see Enroll Surface Hub into MDM management

Manage Surface Hub settings with Intune

The foundational building block of policy settings management in Intune and other MDM providers is the XML-based Open Mobile Alliance-Device Management (OMA-DM) protocol. Windows implements OMA-DM XML via one of many available Configuration service providers (CSPs) with names like AccountManagement CSP, DeviceStatus CSP, WiFi-CSP, and so on. For a complete list, refer to CSPs supported in Microsoft Surface Hub.

Microsoft Intune and other MDM providers use CSPs to deliver a UI that enables you to configure policy settings within Configuration profiles. Intune uses the Surface Hub CSP for its built-in template — **Device restrictions (Windows 10 Team)** — letting you configure basic settings such as preventing Surface Hub from "waking up" whenever anyone moves nearby within its proximity range. To manage Hub settings and features outside of Intune's built-in profile, you'll need to use a custom profile, as shown below.

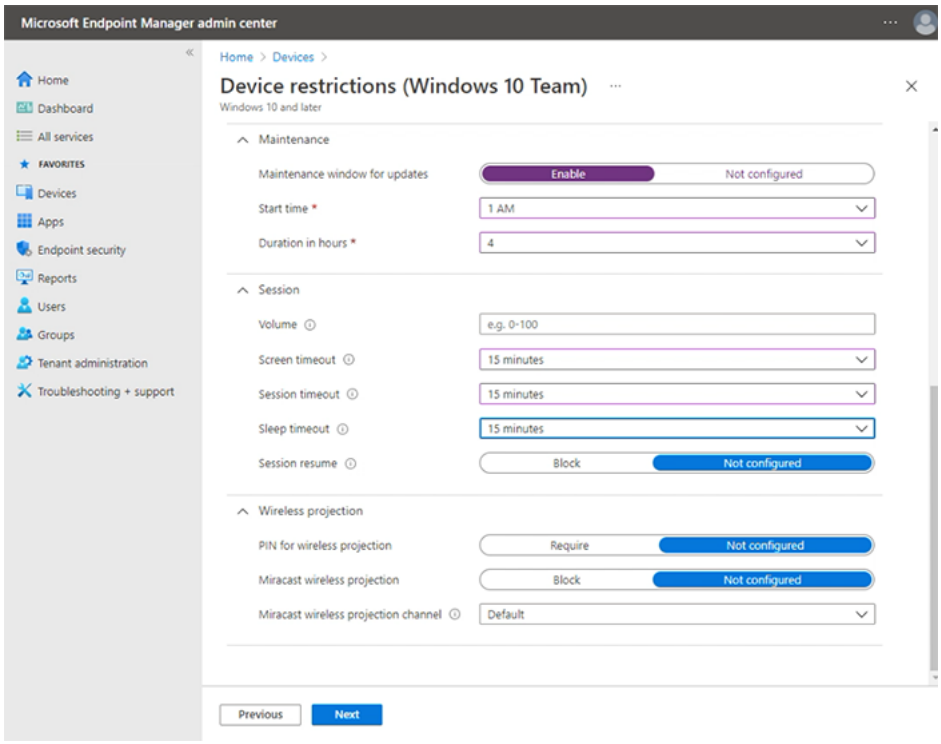
To summarize, options to configure and manage policy settings within Intune include the following:

- **Create a Device restriction profile.** Use Intune's built-in Surface Hub template and configure settings directly in the Intune UI. See Create device restriction profile.
- **Create a Device configuration profile.** Select a template focused on a specific feature or technology such as Microsoft Defender or security certificates. See Create Device configuration profile.
- **Create a Custom configuration profile.** Extend your scope of management using an OMA Uniform Resource Identifier (OMA URI) from any of the CSPs supported in Microsoft Surface Hub. See Create custom configuration profile.

> **Note**
>
> Profiles should be assigned to device groups containing the enrolled Surface Hub devices.

Create Device restriction profile

1. Sign in to **Microsoft Intune admin center**, select **Devices** > **Configuration profiles** > **+ Create profile**.
2. Under **Platform**, select **Windows 10 and later** >
3. Under **Profile type,** select **Templates** and then select **Device restrictions (Windows 10 Team)**
4. Select **Create**, add a name and then select **Next.**
5. You can now browse and choose from preset device restriction settings for Surface Hub across the following categories: Apps and experience, Azure operational insights, Maintenance, Session, and Wireless projection. The example shown in the following figure specifies a 4-hour maintenance window and a 15 minute timeout for screen, sleep and session resume.



For more information about creating and managing profiles, see Restrict devices features using policy in Microsoft Intune.

For more information about how to manage Surface Hub features and settings, see Windows 10 Team settings to allow or restrict features on Surface Hub using Intune

Create Device configuration profile

1. Sign in to **Microsoft Intune admin center**, select **Devices** > **Configuration profiles** > **+ Create profile**.
2. Under **Platform**, select **Windows 10 and later** >
3. Under **Profile type**, select **Templates** and choose from the following templates supported on Surface Hub:
   - Device restrictions (Windows 10 Team), as described in the previous section.
   - Microsoft Defender for Endpoint (Windows 10 Desktop)
   - PKCS certificate
   - PKCS imported certificate
   - SCEP certificate
   - Trusted certificate

Create Custom configuration profile

You can extend the scope of management by creating a custom profile using an OMA URI from any of the CSPs supported in Microsoft Surface Hub. Each setting in a CSP has a corresponding OMA-URI that you can set by using custom configuration profiles in Intune. For details on the CSPs supported by Surface Hub, you can reference the following resources:

- Configuration service provider support
- Policy CSPs supported by Microsoft Surface Hub
- SurfaceHub CSP

> **Note**
>
> Managing the device account using settings from **SurfaceHub CSP** is not currently possible with Intune and requires using a third-party MDM provider.

To implement CSP-based policy settings, begin by generating an OMA URI and then add it to a custom configuration profile in Intune.

Generate OMA URI for target setting

To generate the OMA URI for any setting:

1. In the CSP documentation, identify the root node of the CSP. Generally, this looks like **./Vendor/MSFT/NameOfCSP**.
    - **Example:** The root node of the SurfaceHub CSP is **./Vendor/MSFT/SurfaceHub**.
2. Identify the node path for the setting you want to use.
    - **Example:** The node path for the setting to enable wireless projection is **InBoxApps/WirelessProjection/Enabled**.
3. Append the node path to the root node to generate the OMA URI.
    - **Example:** The OMA URI for the setting to enable wireless projection is **./Vendor/MSFT/SurfaceHub/InBoxApps/WirelessProjection/Enabled.**
4. The data type is also stated in the CSP documentation. The most common data types are:
    - char (String)
    - int (Integer)
    - bool (Boolean)

Add OMA URI to Custom configuration profile

1. In Endpoint Manager, select **Devices** > **Configuration profiles** > **Create profile**.
2. Under Platform select **Windows 10 and later.** Under Profile, select **Custom**, and then select **Create.**
3. Add a name and optional description and then select **Next.**
4. Under **Configuration settings** > **OMA-URI Settings**, select **Add**.

Microsoft Teams and Skype for Business settings

This section highlights Teams and Skype for Business settings that you can manage via Intune or other MDM provider. This includes:

- Quality of Service (QoS)
- Manage Teams-specific features

Quality of Service settings

To ensure optimal video and audio quality on Surface Hub, add the following QoS settings to the device.

Name	Description	OMA-URI	Type	Value
Audio Ports	Audio Port range	./Device/Vendor/MSFT/NetworkQoSPolicy/Audio/SourcePortMatchCondition	String	50000-50019
Audio DSCP	Audio ports marking	./Device/Vendor/MSFT/NetworkQoSPolicy/Audio/DSCPAction	Integer	46
Video Ports	Video Port range	./Device/Vendor/MSFT/NetworkQoSPolicy/Video/SourcePortMatchCondition	String	50020-50039
Video DSCP	Video ports marking	./Device/Vendor/MSFT/NetworkQoSPolicy/Video/DSCPAction	Integer	34
Sharing Ports	Sharing Port range	./Device/Vendor/MSFT/NetworkQoSPolicy/Sharing/SourcePortMatchCondition	String	50040-50059
Sharing DSCP	Sharing ports marking	./Device/Vendor/MSFT/NetworkQoSPolicy/Sharing/DSCPAction	Integer	18

> **Note**
>
> The table shows default port ranges. Administrators may change the port ranges in the Skype for Business and Teams control panel.

Manage Teams-specific features

You can create a Custom configuration profile to manage Teams Coordinated Meetings, Proximity Join, and other features. To learn more, see Manage Microsoft Teams configuration on Surface Hub.

Changing default app for meetings & calls

The default app for meetings & calls on the Surface Hub varies depending on how you install Windows 10 Team 2020 Update (aka Windows 10 20H2 Team edition). If you re-image a Surface Hub to Windows 10 20H2, Microsoft Teams will be set as the default, with Skype

for Business not available (Mode 1). If you upgrade your Hub from an earlier OS version, Skype for Business will remain as the default, with Teams functionality available (Mode 0) unless you had already configured Teams as your default.

To change the default installation, use a custom profile to set the Teams Meeting Mode as follows:

- Mode 0 — Skype for Business with Microsoft Teams functionality for scheduled meetings.
- Mode 1 — Microsoft Teams only.

Name	Description	OMA-URI	Type	Value
Teams App ID	App name	./Vendor/MSFT/SurfaceHub/Properties/VtcAppPackageId	String	Microsoft.MicrosoftTeamsforSurfaceHub_8wekyb3d8bbwe!Team
Teams App Mode	Teams mode	./Vendor/MSFT/SurfaceHub/Properties/SurfaceHubMeetingMode	Integer	0 or 1

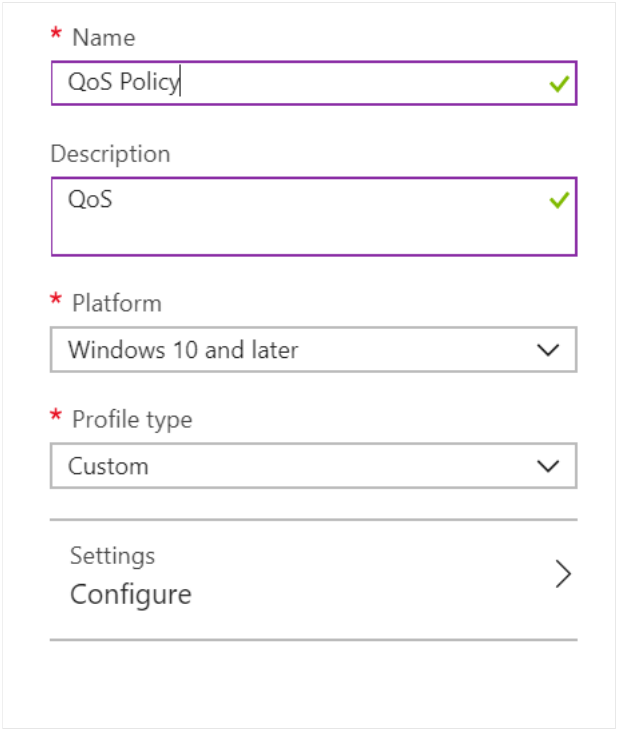
Implement Quality of Service (QoS)

Quality of Service (QoS) is a combination of network technologies that allows the administrators to optimize the experience of real time audio/video and application sharing communications.

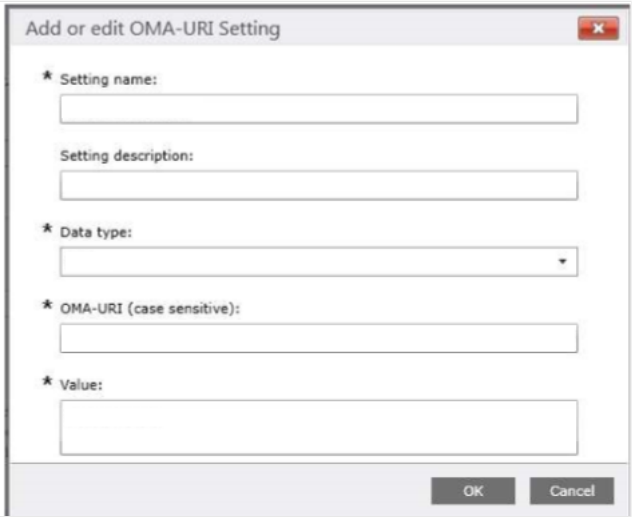
Configuring QoS for Teams or Skype for Business on the Surface Hub can be done using your MDM provider or through a provisioning package.

This procedure explains how to configure QoS for Surface Hub using Microsoft Intune.

1. In Intune, create a custom policy.



2. In **Custom OMA-URI Settings**, select **Add**. For each setting that you add, you will enter a name, description (optional), data type, OMA-URI, and value.



3. Add the following custom OMA-URI settings:

Name	Data type	OMA-URI ./Device/Vendor/MSFT/NetworkQoSPolicy	Value
Audio Source Port	String	/HubAudio/SourcePortMatchCondition	Get the values from your Skype administrator
Audio DSCP	Integer	/HubAudio/DSCPAction	46
Video Source Port	String	/HubVideo/SourcePortMatchCondition	Get the values from your Skype administrator
Video DSCP	Integer	/HubVideo/DSCPAction	34
Audio Process Name	String	/HubAudio/AppPathNameMatchCondition	Microsoft.PPISkype.Windows.exe
Video Process Name	String	/HubVideo/AppPathNameMatchCondition	Microsoft.PPISkype.Windows.exe

> ⓘ **Important**
>
> Each **OMA-URI** path begins with `./Device/Vendor/MSFT/NetworkQoSPolicy`. The full path for the audio source port setting, for example, will be `./Device/Vendor/MSFT/NetworkQoSPolicy/HubAudio/SourcePortMatchCondition`.

4. When the policy has been created, deploy it to Surface Hub.

> ⚠ **Warning**
>
> Currently, you cannot configure the setting **IPProtocolMatchCondition** in the NetworkQoSPolicy CSP. If this setting is configured, the policy will fail to apply.

Admin group management for Surface Hub

Article • 01/10/2023 • Applies to: Surface Hub, Surface Hub 2S

Every Surface Hub can be configured locally using the Settings app on the device. To prevent unauthorized users from changing settings, the Settings app requires admin credentials to open the app.

Admin Group Management

You can set up administrator accounts for the device in the following ways:

- Create a local admin account
- Domain join the device to Active Directory
- Azure AD join the device
- Configure non-Global Admin accounts on Azure AD joined devices (Surface Hub 2S)

Create a local admin account

To create a local admin, choose to use a local admin during first run. This will create a single local admin account on the Surface Hub with the username and password of your choice. Use these credentials to open the Settings app.

Note that the local admin account information is not backed by any directory service. We recommend you only choose a local admin if the device does not have access to Active Directory (AD) or Azure Active Directory (Azure AD). If you decide to change the local admin's password, you can do so in Settings. However, if you want to change from using the local admin account to using a group from your domain or Azure AD tenant, then you'll need to reset the device and go through the first-time program again.

Domain join the device to Active Directory

You can domain join the Surface Hub to your AD domain to allow users from a specified security group to configure settings. During first run, choose to use Active Directory Domain Services. You'll need to provide credentials that are capable of joining the domain of your choice, and the name of an existing security group. Anyone who is a member of that security group can enter their credentials and unlock Settings.

What happens when you domain join your Surface Hub?

Surface Hubs use domain join to:

- Grant admin rights to members of a specified security group in AD.
- Backup the device's BitLocker recovery key by storing it under the computer object in AD. See Save your BitLocker key for details.
- Synchronize the system clock with the domain controller for encrypted communication

Surface Hub does not support applying Group Policy or certificates from the domain controller.

> **Note**
>
> If your Surface Hub loses trust with the domain (for example, if you remove the Surface Hub from the domain after it is domain joined), you won't be able to authenticate into the device and open up Settings. If you decide to remove the trust relationship of the Surface Hub with your domain, **reset the device** first.

Azure AD join the device

You can Azure Active Directory (Azure AD) to join the Surface Hub to allow IT pros from your Azure AD tenant to configure settings. During first run, choose to use Microsoft Azure Active Directory. You will need to provide credentials that are capable of joining the Azure AD tenant of your choice. After you successfully Azure AD join, the appropriate people will be granted admin rights on the device.

By default, all **global administrators** will be given admin rights on an Azure AD joined Surface Hub. With **Azure AD Premium** or **Enterprise Mobility Suite (EMS)**, you can add additional administrators:

1. In the Azure classic portal, click **Active Directory**, and then click the name of your organization's directory.
2. On the **Configure** page, under **Devices** > **Additional administrators on Azure AD joined devices**, click **Selected**.
3. Click **Add**, and select the users you want to add as administrators on your Surface Hub and other Azure AD joined devices.
4. When you have finished, click the checkmark button to save your change.

What happens when you Azure AD join your Surface Hub?

Surface Hubs use Azure AD join to:

- Grant admin rights to the appropriate users in your Azure AD tenant.
- Backup the device's BitLocker recovery key by storing it under the account that was used to Azure AD join the device. See Save your BitLocker key for details.

Automatic enrollment via Azure Active Directory join

Surface Hub now supports the ability to automatically enroll in Intune by joining the device to Azure Active Directory.

For more information, see Set up enrollment for Windows devices.

Which should I choose?

If your organization is using AD or Azure AD, we recommend you either domain join or Azure AD join, primarily for security reasons. People will be able to authenticate and unlock Settings with their own credentials, and can be moved in or out of the security groups associated with your domain.

Option	Requirements	Which credentials can be used to access the Settings app?
Create a local admin account	None	The user name and password specified during first run
Domain join to Active Directory (AD)	Your organization uses AD	Any AD user from a specific security group in your domain
Azure Active Directory (Azure AD) join the device	Your organization uses Azure AD Basic	Global administrators only
	Your organization uses Azure AD Premium or Enterprise Mobility Suite (EMS)	Global administrators and additional administrators

Configure non-Global Admin accounts on Azure AD-joined devices

For Surface Hub v1 and Surface Hub 2S devices joined to Azure AD, Windows 10 Team 2020 Update lets you limit admin permissions to management of the Settings app on Surface Hub. This enables you to scope admin permissions for Surface Hub only and

prevent potentially unwanted admin access an entire Azure AD domain. To learn more, see Configure non-Global Admin accounts on Surface Hub.

Manage Microsoft Edge on Surface Hub

Article • 01/25/2023 • Applies to: Surface Hub, Surface Hub 2S

Use Microsoft Edge browser policies to configure browser settings in Microsoft Edge via any of the following methods:

- Microsoft Intune
- Your preferred Mobile Device Management (MDM) provider that supports ADMX Ingestion
- Provisioning packages using ADMX Ingestion in Windows Configuration Designer

> **Tip**
>
> The swipe down from top of screen gesture to exit full-screen mode requires two fingers with the new Microsoft Edge. The exit full-screen action is also available in the context menu displayed after a long-press touch.

Default Microsoft Edge policies for Surface Hub

Microsoft Edge is preconfigured with the following policy settings to provide an optimized experience for Surface Hub.

> **Tip**
>
> It's recommended to retain the default value for these policy settings.

Policy setting	Recommended experience	Default value
AutoImportAtFirstRun	Don't automatically import datatypes and settings from Microsoft Edge Legacy. This configuration avoids changing signed-in users' profiles with shared settings from the Surface Hub.	4
BackgroundModeEnabled	Allow Microsoft Edge processes to keep running in the background even after the last browser window is closed, enabling faster access to web apps during a session.	1

Policy setting	Recommended experience	Default value
BrowserAddProfileEnabled	Don't allow users to create new profiles in Microsoft Edge, simplifying the browsing and signed-in experience.	0
BrowserGuestModeEnabled	Enables only one user to sign-in to Microsoft Edge, simplifying the browsing and signed-in experience	0
BrowserSignin	Enables users to enjoy single sign-on (SSO) in Microsoft Edge. When users are signed into Surface Hub, their credentials can flow to supported websites without requiring them to reauthenticate.	1
ExtensionInstallBlockList	Prevents non-admin users from installing new extensions in Microsoft Edge. To configure a list of extensions to be installed by default, use ExtensionInstallForcelist.	*
HideFirstRunExperience	Hides the first run experience and splash screen that's normally shown when users run Microsoft Edge for the first time.	1
InPrivateModeAvailability	Disables InPrivate mode. Since End Session already clears browsing data, disabling InPrivate mode simplifies the browsing and signed-in experience.	1
NewTabPageSetFeedType	Shows the Microsoft 365 feed experience on new tab pages. When users are signed into Surface Hub, this tab display enables fast access to files and content on Microsoft 365.	1
NonRemovableProfileEnabled	When users are signed into Surface Hub, a non-removable profile is created using their organizational account, simplifying the SSO experience.	1
PrintingEnabled	Disables printing in Microsoft Edge. Surface Hub doesn't support printing.	0
ProActiveAuthEnabled	Enables Microsoft Edge to proactively authenticate signed-in users with Microsoft services, simplifying the SSO experience.	1
PromptForDownloadLocation	Automatically saves files to the Downloads folder, rather than asking users where to save the file, simplifying the browsing experience.	0

Tip

Deployable progressive web apps (PWAs) are now supported on the Windows 10 Team operating system. To learn more, see **Install Progressive Web Apps on Surface Hub**.

Configure Microsoft Edge updates

By default, Microsoft Edge is updated automatically. Use Microsoft Edge update policies to configure settings for Microsoft Edge Update. Surface Hub doesn't support the **CreateDesktopShortcut** policy setting as Surface Hub doesn't use desktop shortcuts.

> **Tip**
>
> Microsoft Edge requires connectivity to the Internet to support its features. Add the **necessary domain URLs** to the Allow list to ensure communications through firewalls and other security mechanisms.

Related links

- Microsoft Edge documentation

Monitor Surface Hub

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

Monitoring for Surface Hub devices is enabled through Azure Monitor (formerly Microsoft Operations Management Suite or OMS). To get started, refer to Monitor Surface Hubs with Azure Monitor to track their health.

Related topics

- Manage Surface Hub

Manage Windows Update on Surface Hub

Article • 02/16/2023

New releases of the Surface Hub operating system are published through Windows Update, just like releases of Windows 10 or Windows 11. This page explains best practices for managing updates for Surface Hub devices.

Windows Update for Business

Windows Update for Business is a set of features designed to provide enterprises additional control over how and when Windows Update installs releases, while reducing device management costs. Using this method, Surface Hubs are directly connected to Microsoft's Windows Update service.

- Receive updates directly from Microsoft's Windows Update service, with no additional infrastructure required.
- Defer updates to provide additional time for testing and evaluation.
- Deploy updates to select groups of devices.
- Define maintenance windows for installing updates.

> **Tip**
>
> Use peer-to-peer content sharing to reduce bandwidth issues during updates. See **Optimize Windows update delivery** for details.

> **Note**
>
> Surface Hub does not currently support rolling back updates.

Surface Hub servicing model

Surface Hub uses the Windows servicing model, referred to as Windows as a Service (WaaS). Traditionally, new features were added only in new versions of Windows that were released every few years. Each new version required lengthy and expensive processes to deploy in an organization. As a result, end users and organizations don't

frequently enjoy the benefits of new innovation. The goal of Windows as a Service is to continually provide new capabilities while maintaining a high level of quality.

Microsoft publishes two types of Surface Hub releases broadly on an ongoing basis:

- **Feature updates** - Updates that install the latest new features, experiences, and capabilities. Microsoft expects to publish two new feature updates per year.
- **Quality updates** - Updates that focus on the installation of security fixes, drivers, and other servicing updates. Microsoft expects to publish one cumulative quality update per month.

In order to improve release quality and simplify deployments, all new releases that Microsoft publishes for Windows 10 or Windows 11, including Surface Hub, will be cumulative. This means new feature updates and quality updates will contain the payloads of all previous releases (in an optimized form to reduce storage and networking requirements), and installing the release on a device will bring it completely up to date. Also, unlike earlier versions of Windows, you cannot install a subset of the contents of a Windows 10 quality update. For example, if a quality update contains fixes for three security vulnerabilities and one reliability issue, deploying the update will result in the installation of all four fixes.

The Surface Hub operating system receives updates on the Semi-Annual Channel. Like other editions of Windows 10 or Windows 11, the servicing lifetime is finite. You must install new feature updates on machines running these branches in order to continue receiving quality updates.

For more information on Windows as a Service, see Overview of Windows as a service.

Use Windows Update for Business

Surface Hubs, like all Windows 10 devices, include **Windows Update for Business (WUfB)** to enable you to control how your devices are being updated. Windows Update for Business helps reduce device management costs, provide controls over update deployment, offer quicker access to security updates, as well as provide access to the latest innovations from Microsoft on an ongoing basis. For more information, see Manage updates using Windows Update for Business.

> **ⓘ Important**
>
> Microsoft generally releases one mandatory Windows security update per month (released on the 2nd Tuesday and often referred to as a "B" release). Together with out-of-band security updates, these are the only updates made available to devices

using WUfB. However, Surface Hub improvements are generally delivered through optional non-security updates on the 3rd Tuesday of each month ("C" release). As a result, customers using Windows Update for Business with their Surface Hubs will have wait until the following month's "B" release to see the latest improvements on these devices.

To set up Windows Update for Business:

1. Group Surface Hub into deployment rings
2. Configure when Surface Hub receives updates.

> **Note**
>
> You can use Microsoft Intune, Microsoft Endpoint Configuration Manager, or a supported third-party MDM provider to set up WUfB. **Walkthrough: use Microsoft Intune to configure Windows Update for Business.**

Group Surface Hub into deployment rings

Use deployment rings to control when updates roll out to your Surface Hubs, giving you time to validate them. For example, you can update a small pool of devices first to verify quality before a broader roll-out to your organization. Depending on who manages Surface Hub in your organization, consider incorporating Surface Hub into the deployment rings that you've built for your other Windows 10 or Windows 11 devices. For more information about deployment rings, see Prepare servicing strategy for Windows client updates.

See the following table for examples of deployment rings.

Deployment ring	Ring size	Servicing branch	Deferral for feature updates	Deferral for quality updates (security fixes, drivers, and other updates)	Validation step
Preview (e.g. non-critical or test devices)	Small	Windows Insider Preview	None.	None.	Manually test and evaluate new functionality. Pause updates if there are issues.

Deployment ring	Ring size	Servicing branch	Deferral for feature updates	Deferral for quality updates (security fixes, drivers, and other updates)	Validation step
Release (e.g. devices used by select teams)	Medium	Semi-annual channel	None.	None.	Monitor device usage and user feedback. Pause updates if there are issues.
Broad deployment (e.g. most of the devices in your organization)	Large	Semi-annual channel	120 days after release.	7-14 days after release.	Monitor device usage and user feedback. Pause updates if there are issues.
Mission critical (e.g. devices in executive boardrooms)	Small	Semi-annual channel	180 days after release (maximum deferral for feature updates).	30 days after release (maximum deferral for quality updates).	Monitor device usage and user feedback.

Configure when Surface Hub receives updates

Once you've determined deployment rings for your Surface Hubs, configure update deferral policies for each ring:

- To defer feature updates, set an appropriate Update/DeferFeatureUpdatesPeriodInDays policy for each ring.
- To defer quality updates, set an appropriate Update/DeferQualityUpdatesPeriodInDays policy for each ring.

> ⓘ **Note**
>
> If you encounter issues during the update rollout, you can pause updates using **Update/PauseFeatureUpdates** and **Update/PauseQualityUpdates**.

If you use a proxy server or other method to block URLs

Add the following Windows update trusted site URLs to the "allow list":

- `http(s)://*.update.microsoft.com`

- `http://download.windowsupdate.com`
- `http://windowsupdate.microsoft.com`

Once the Windows 10 Team Anniversary Update is installed, you can remove these addresses to return your Surface Hub to its previous state.

Maintenance window

To ensure the device is always available for use during business hours, the Surface Hub performs its administrative functions during a specified maintenance window. The Surface Hub automatically installs updates through Windows Update during the maintenance window, and reboots the device 20 minutes before the end of the window.

Surface Hub follows these guidelines to apply updates:

- Install the update during the next maintenance window. If a meeting is scheduled to start during a maintenance window, or the Surface Hub sensors detect that the device is being used, the pending update will be postponed to the following maintenance window.
- If the next maintenance window is past the update's prescribed grace period, the device will calculate the next available slot during business hours using the estimated install time from the update's metadata. It will continue to postpone the update if a meeting is scheduled, or the Surface Hub sensors detect that the device is being used.
- If the next maintenance window is **not** past the update's grace period, the Surface Hub will continue to postpone the update.
- If an additional reboot is needed, the Surface Hub will automatically reboot during the next maintenance window.

> **Tip**
>
> Allow time for updates when you first setup your Surface Hub. For example, a backlog of virus definitions may be available, which should be immediately installed.

A default maintenance window is set for all new Surface Hubs:

- **Start time:** 2:00 AM
- **Duration:** 2 hours

To manually change the maintenance window:

1. Open **Settings** on your Surface Hub.
2. Navigate to **Update & security** > **Windows Update** > **Advanced options**.
3. Under **Maintenance hours**, select **Change**.

To change the maintenance window using MDM, set the **MaintenanceHoursSimple** node in the SurfaceHub configuration service provider. See Manage settings with an MDM provider for more details.

Related topics

- Manage Microsoft Surface Hub
- Surface Hub may install updates and restart outside maintenance hours

Manage EU privacy settings on Surface Hub

Article • 02/16/2023 • Applies to: Surface Hub, Surface Hub 2S

In May 2018, a European privacy law, the General Data Protection Regulation (GDPR), took effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents.

Surface Hub customers concerned about privacy under the new GDPR regulations can manage their device privacy with the following options that are provided by Microsoft:

- **Option 1:** Surface Hub devices in regions enforcing GDPR regulations automatically reduce diagnostic data emission to basic. Customers opting to provide a higher level of diagnostic data can use the Surface Hub Settings application or Mobile Device Management to override the default basic setting.
- **Option 2:** Surface Hub customers who want to remove any existing diagnostic data can download the **Surface Hub Delete Diagnostic Data** application from the Microsoft Store. This app will allow customers to request deletion of associated diagnostic data directly from their Surface Hub device.

Microsoft has extensive expertise in protecting data, championing privacy, and complying with complex regulations, and currently complies with both EU-U.S. Privacy Shield and EU Model Clauses. We believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights. We want to help you focus on your core business while efficiently preparing for the GDPR.

Learn more

- General Data Protection Regulation Summary

Check Surface Hub warranty status

Article • 04/19/2023 • Applies to: Surface Hub, Surface Hub 2S

You can check the warranty status directly from Surface Hub or from the cloud, via the Surface Support for Business Online Service Center or the Microsoft Intune admin center.

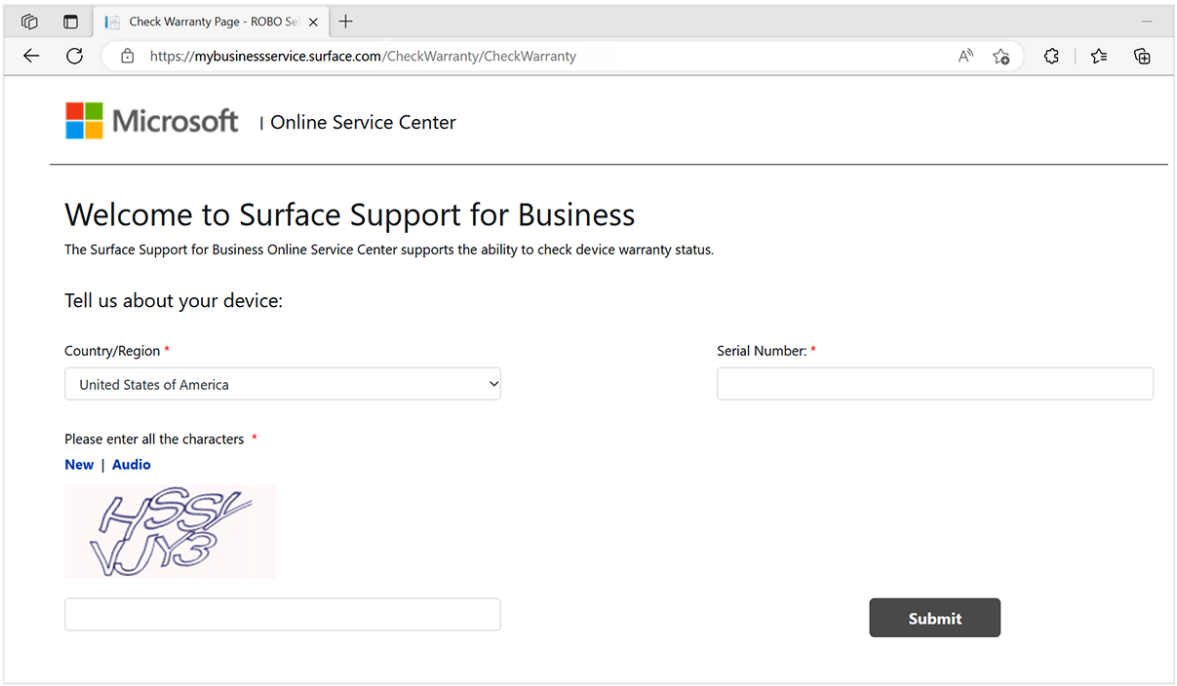
Check warranty status from Surface Hub

1. On Surface Hub, open the Start menu. Select **All Apps** > **Surface** app.
2. Select **Warranty & Services**. Warranty information is displayed.

Check warranty status via Surface Support for Business Online Service Center

1. Go to the Surface Support for Business Online Service Center.

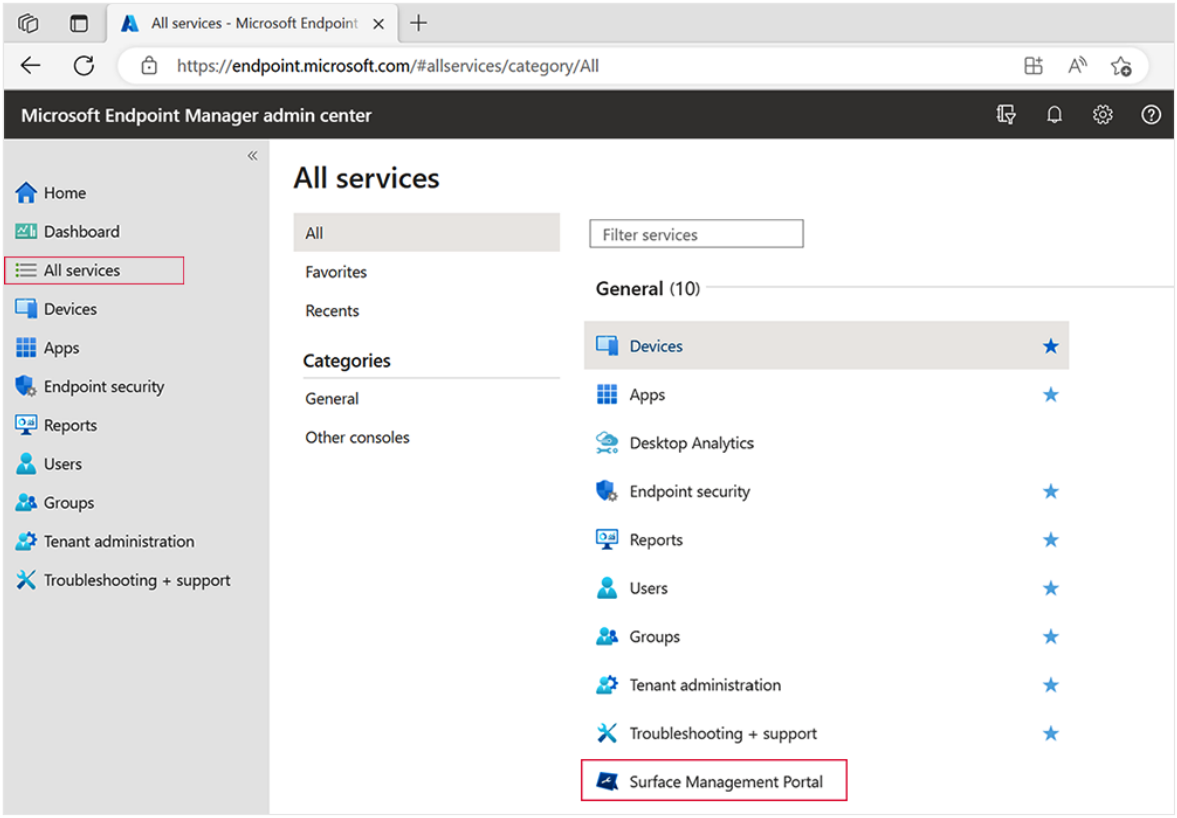
2. Enter the Country/Region and Serial Number. Add the characters shown and select **Submit**.



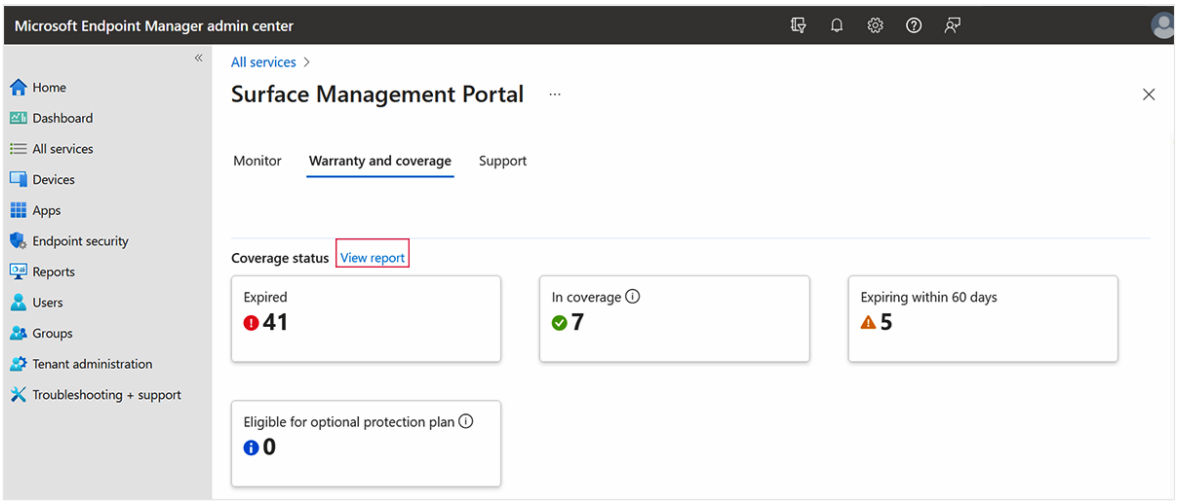
Check warranty status in Surface Management Portal

1. Sign in to the Endpoint Manager Admin Center.

2. Select **All Services** > **Surface Management Portal**. This takes you to the main page of the Surface Management Portal that displays information for all your Surface devices.

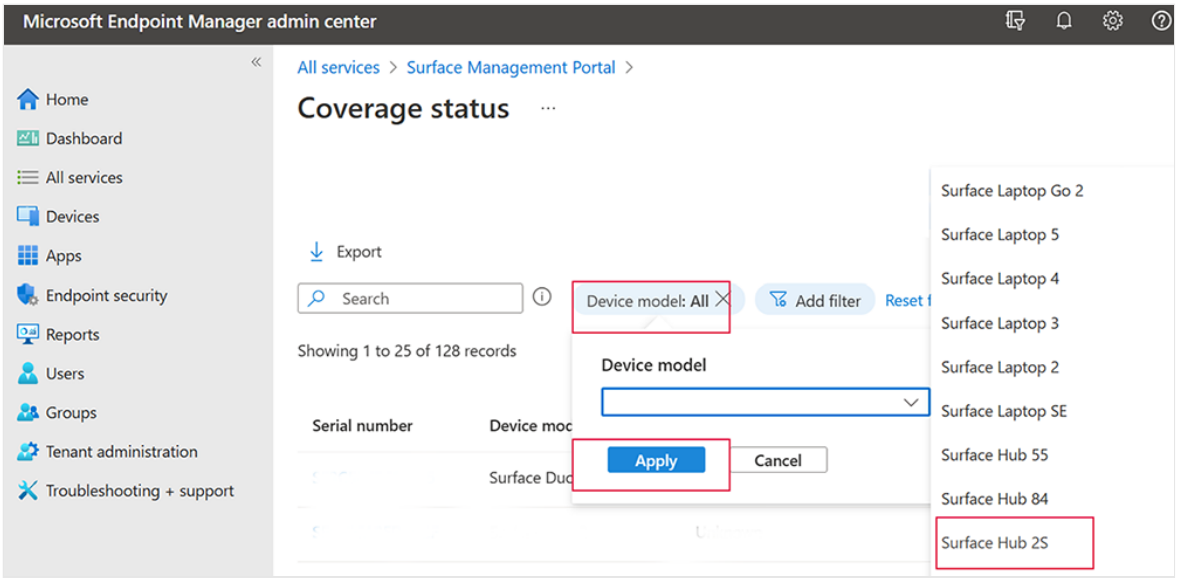


3. Under Warranty and coverage, select **View report** .



4. To filter for Surface Hub devices, select **Add filter**. From the dropdown menu, select **Device model** > **Apply**.

5. After the filter is applied, select **Device model: All**. From the dropdown menu, choose your Surface Hub model and then select **Apply**.


Microsoft Endpoint Manager admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
All services > Surface Management Portal >
Coverage status
Export
Search
Device model: All
Add filter
Showing 1 to 25 of 128 records
Device model
Apply
Cancel
Serial number
Surface Laptop Go 2
Surface Laptop 5
Surface Laptop 4
Surface Laptop 3
Surface Laptop 2
Surface Laptop SE
Surface Hub 55
Surface Hub 84
Surface Hub 2S

Enroll Surface Hub in the Windows Insider Program

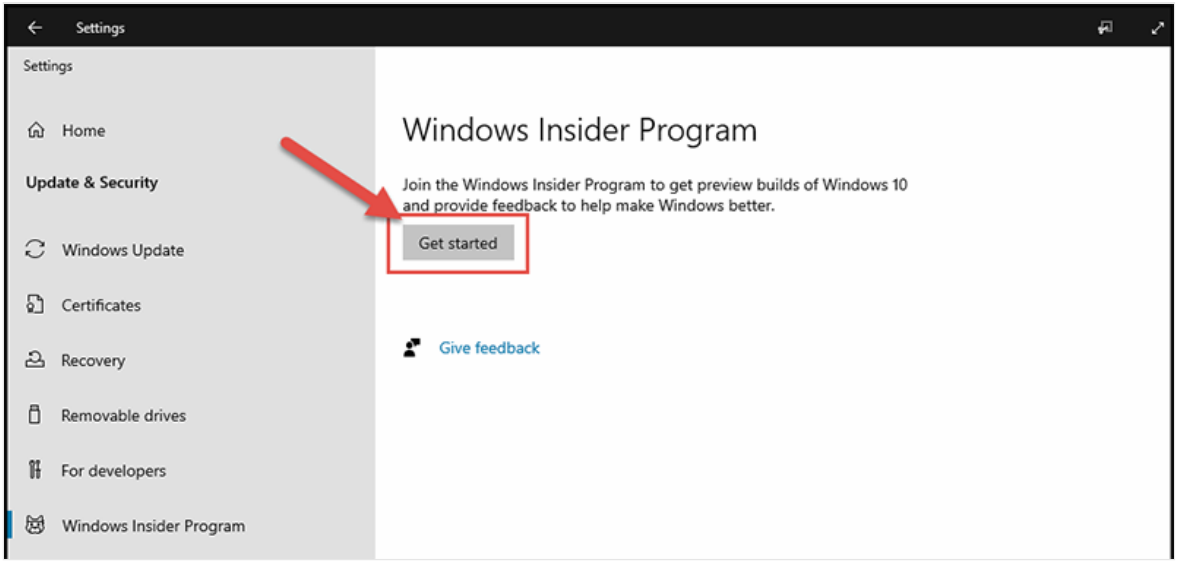
Article • 01/04/2023 • Applies to: Surface Hub, Surface Hub 2S

Be the first to see what's next for Surface Hub in the Windows Insider Program. Join the community and give us your feedback to help make Surface Hub better.

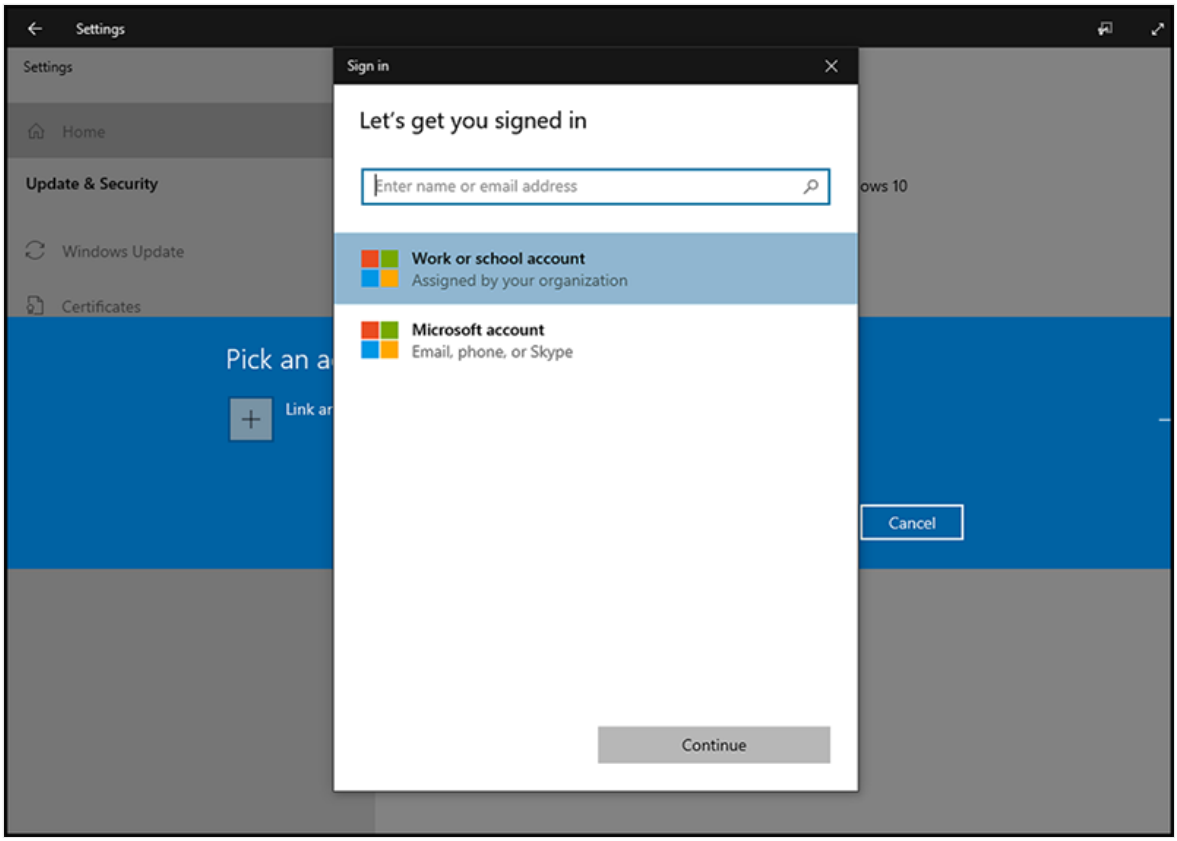
1. Go to https://insider.windows.com/ and register your account for Windows Insider Program.

2. Sign in to **Settings** on Surface Hub with an admin account.

3. Go to **Update & Security**, select **Windows Insider Program** from the left menu, and then select **Get started**.

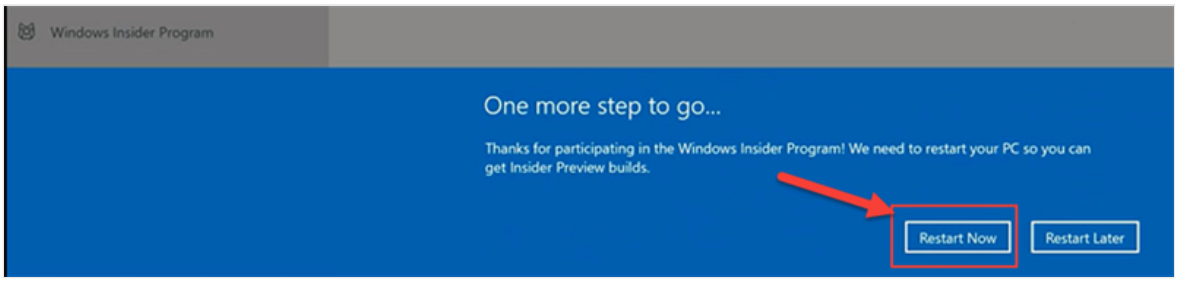


4. Select **Link account** and complete the sign-in process with the account registered with the Windows Insider Program



5. Make sure the Dev Channel is chosen and select **Confirm**.

6. Choose **Restart Now**. Surface Hub is now enrolled in the Windows Insider Program.



7. When Surface Hub restarts, sign restarts, sign back into Settings and go to **Update & Security** > **Windows Update.** Select **Check for updates** to find and start the installation of the Insider Preview.

> ⓘ **Note**
>
> To unenroll Surface Hub from the Windows Insider Program, you must reset the device. To learn more, see **Reset and recovery for Surface Hub 2S**.

Configure Surface Hub Start menu

Article • 04/19/2023

Surface Hub ships with a default Start menu that admins can modify with specific apps to meet organizational requirements. For example, you can install Progressive Web Apps and include them in the Start menu for quick user access at the start of every Hub session.

Overview

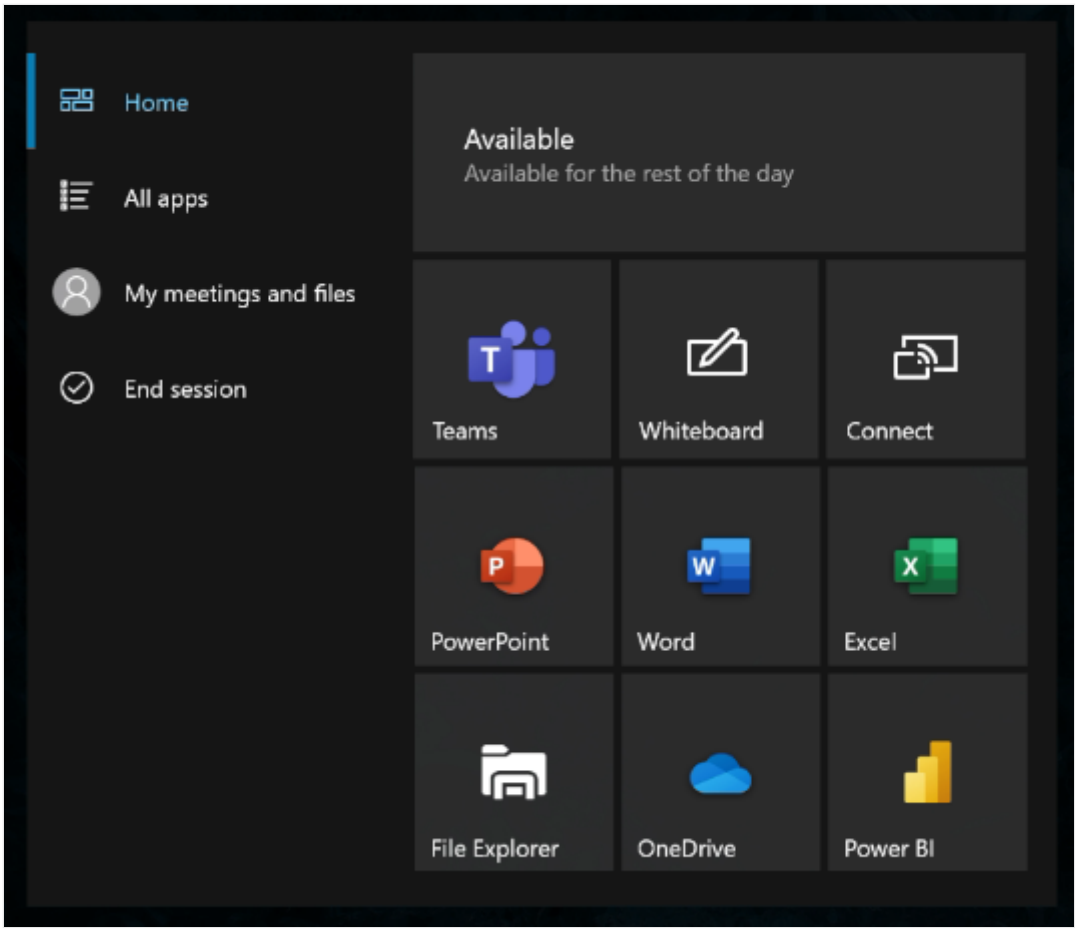
The Surface Hub Start menu is rendered from a Start layout XML file that includes App ID values (AppUserModelID) for default applications such as Microsoft PowerPoint, Word, and Excel. You can add new tiles or replace the default values with the AppUserModelID associated with the apps you wish to display. As described below, use a mobile device management (MDM) provider such as Microsoft Intune to deploy a Start layout device policy containing your modified Start layout XML. To learn more, refer to Manage Surface Hub with an MDM provider.

Differences between Surface Hub and desktop Start menu

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

- You cannot use the Start layout XML to configure the taskbar or the Welcome screen for Surface Hub.
- The Start layout policy should be assigned only to devices, not users.
- The OMA-URI setting to use in the policy is `./Device/Vendor/MSFT/Policy/Config/Start/StartLayout`
- **DesktopApplicationTile** is only supported for Edge and Microsoft Teams. All other Win32 apps are blocked by Code Integrity policy

Default Surface Hub Start menu



The default Start menu is rendered by the following Start XML layout.

XML

```
<LayoutModificationTemplate Version="1"
xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification">
  <LayoutOptions StartTileGroupCellWidth="8" />
  <DefaultLayoutOverride>
    <StartLayoutCollection>
      <defaultlayout:StartLayout GroupCellWidth="8"
xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayo
ut">
        <start:Group Name=""
xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout">
        <start:DesktopApplicationTile
            DesktopApplicationID="MSEdge"
            Size="2x2"
            Row="0"
            Column="0"/>
        <start:Tile
            AppUserModelID="Microsoft.Getstarted_8wekyb3d8bbwe!App"
            Size="4x2"
            Row="0"
            Column="2"/>
        <start:Tile

AppUserModelID="Microsoft.Office.PowerPoint_8wekyb3d8bbwe!Microsoft.pptim"
            Size="2x2"
```

```
            Row="2"
            Column="0"/>
        <start:Tile

AppUserModelID="Microsoft.Office.Word_8wekyb3d8bbwe!Microsoft.Word"
            Size="2x2"
            Row="2"
            Column="2"/>
        <start:Tile

AppUserModelID="Microsoft.Office.Excel_8wekyb3d8bbwe!Microsoft.Excel"
            Size="2x2"
            Row="2"
            Column="4"/>
        <start:Tile
            AppUserModelID="c5e2524a-ea46-4f67-841f-
6a9465d9d515_cw5n1h2txyewy!App"
            Size="2x2"
            Row="4"
            Column="0"/>
        <start:Tile
            AppUserModelID="microsoft.microsoftskydrive_8wekyb3d8bbwe!App"
            Size="2x2"
            Row="4"
            Column="2"/>
        <start:Tile

AppUserModelID="Microsoft.MicrosoftPowerBIForWindows_8wekyb3d8bbwe!Microsoft
.MicrosoftPowerBIForWindows"
            Size="2x2"
            Row="4"
            Column="4"/>
        </start:Group>
      </defaultlayout:StartLayout>
    </StartLayoutCollection>
  </DefaultLayoutOverride>
</LayoutModificationTemplate>
```

Modify default Start menu

Customize the Start menu by modifying the **Start:Tile** elements of the XML. Surface Hub supports a maximum of 12 tiles. Do not adjust the default width: **GroupCellWidth="8"**.

This example adds the following Progressive Web Apps to the default XML layout. See Appendix A for the modified Start layout XML file containing these PWAs.

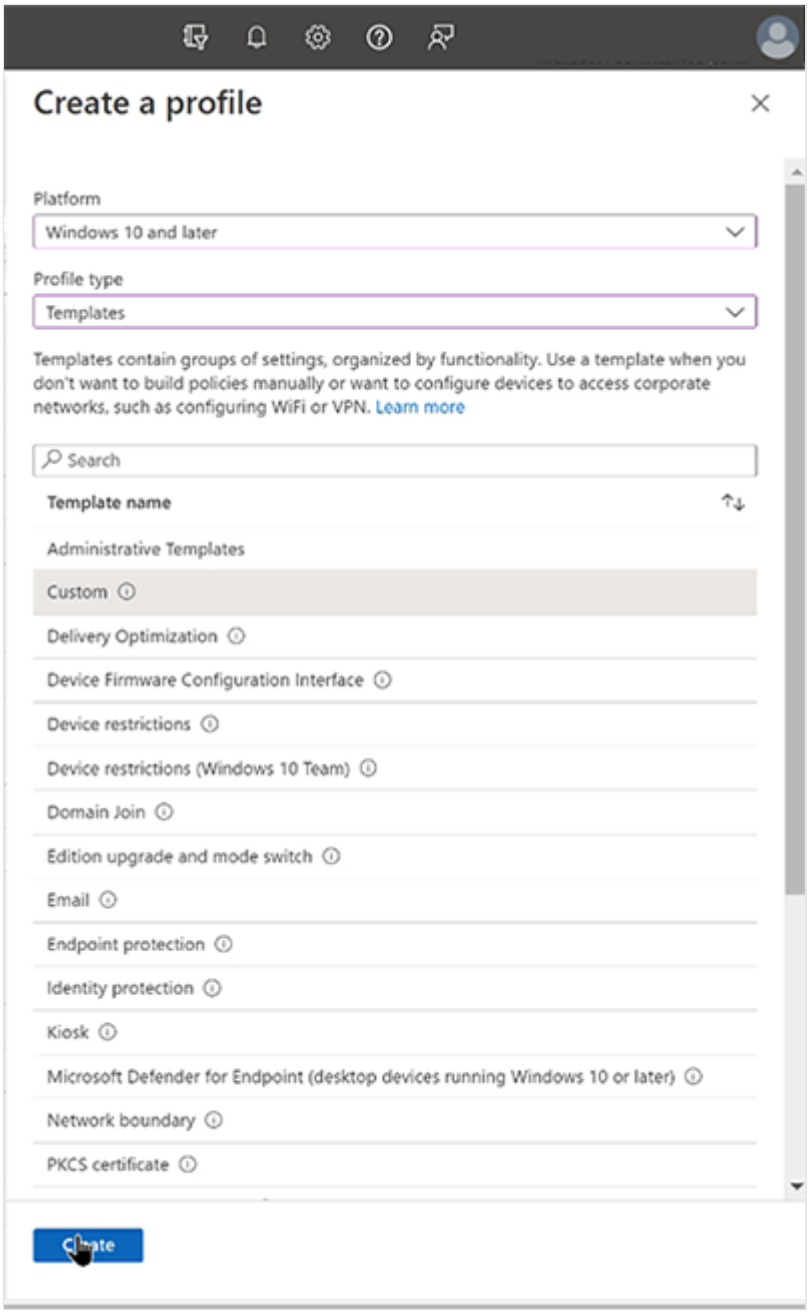
App	AppUserModelID
WebEx	signin.webex.com-8846C236_2aab1d9x9fqba!App
Zoom	zoom.us-F576B427_j0dtdqw38r40m!App

App	AppUserModelID
YouTube	www.youtube.com-756BE99A_pd8mbgmqs65xy!App

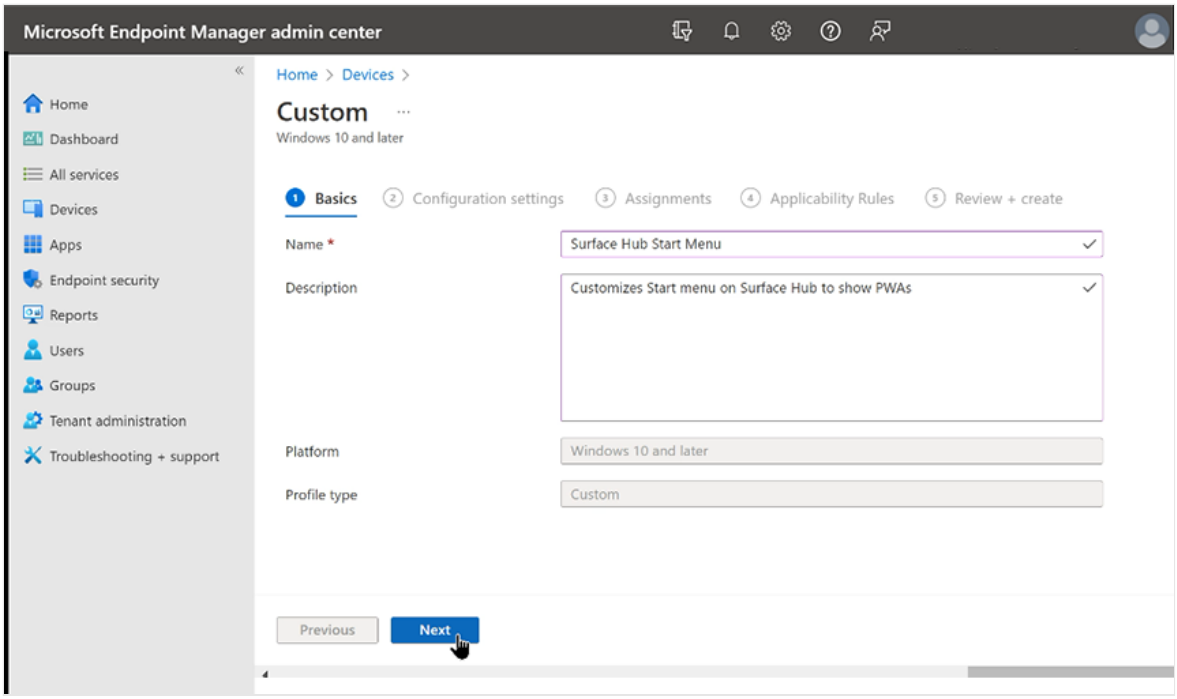
> **Tip**
>
> See **Appendix B** for instructions on obtaining the AppUserModelID for other apps installed on Surface Hub.

Deploy modified Start menu to Surface Hub

1. Save your modified Start menu XML to a separate PC.
2. Sign in to the Intune portal at **Microsoft Intune admin center**.
3. Go to **Devices** > **Configuration Policies** > **Create profile**.
4. Under Platform, select **Windows 10 and later**. Under Profile type, select **Templates**. Under Template name, select **Custom** and choose **Create**.



5. On the configuration settings page, select **Add.** Enter a name and optional description. Select **Next**.



6. For OMA-URI, enter the following string:

```
./Device/Vendor/MSFT/Policy/Config/Start/StartLayout
```

7. For Data type, select **String (XML file) and** open your modified Start layout XML file. Select **Save** and then click **Next**.

Assign Start layout policy

The Configuration profile **must** be assigned to devices and targeted to the device URI. Do not use: `./User/Vendor/MSFT/Policy/Config/Start/StartLayout`.

1. On the Assignments page, under **Included groups**, select **Add groups**.

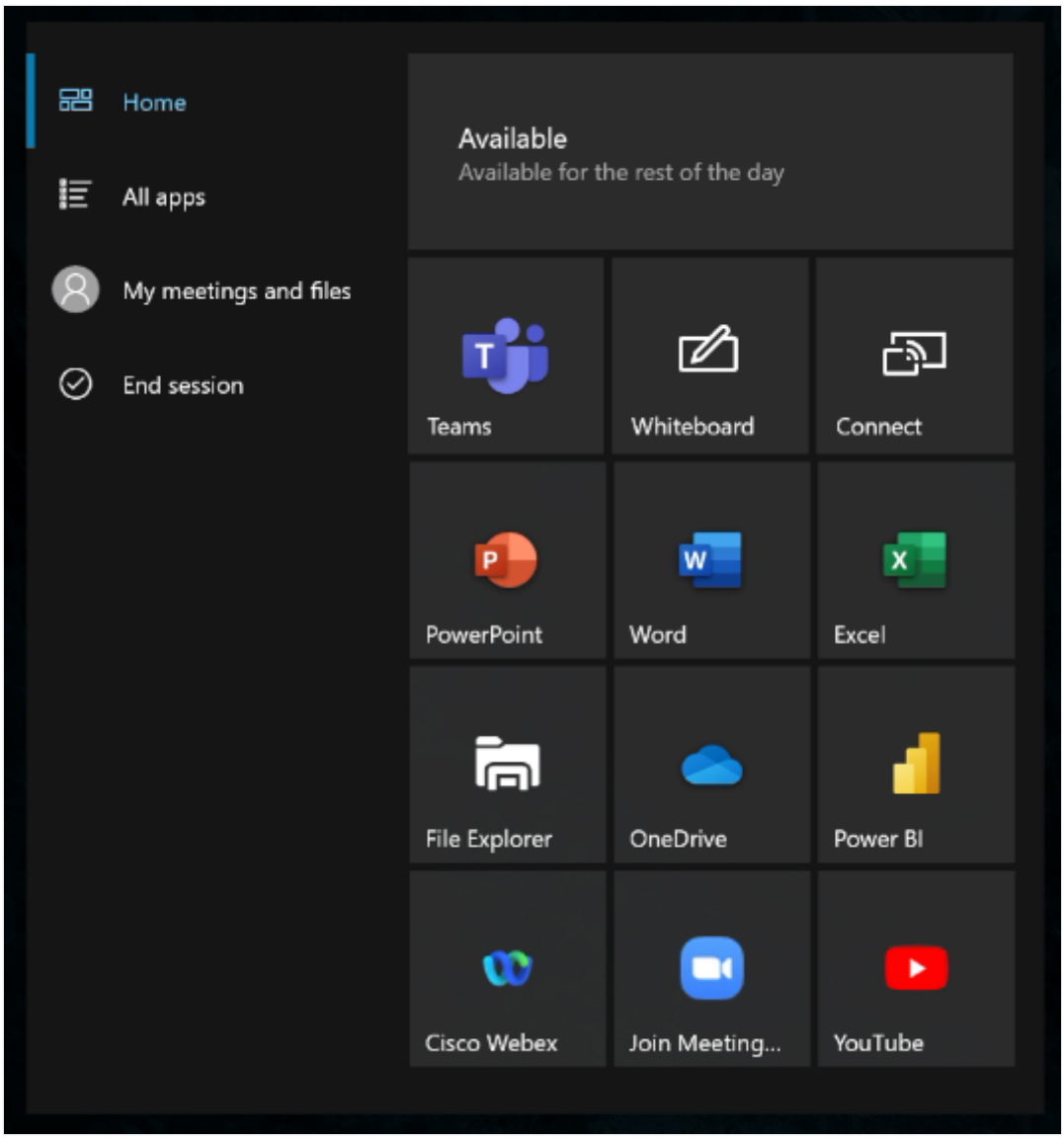
2. Under **Select groups to include**, enter the name of a group containing the Surface Hubs you wish to target, choose **Select**, and then click **Next**. To learn more about assigning a Configuration profile to a group, see Add groups to organize users and devices.

3. On the Applicability Rules page, enter optional criteria if desired. Otherwise, select **Next**.

4. Review the Configuration profile and select **Create**.

5. To apply the Configuration profile immediately, select **Devices** > **All devices** and find the Surface Hub you targeted. Open its Overview pane, and select **Sync**.

6. Once applied, you will see the modified Start menu on your Surface Hub.



Appendix A: Surface Hub Start menu modified for Progressive Web Apps

The following modified Start layout XML includes PWAs for WebEx, Zoom, and YouTube.

XML

```
<LayoutModificationTemplate Version="1"
xmlns="http://schemas.microsoft.com/Start/2014/LayoutModification">
  <LayoutOptions StartTileGroupCellWidth="8" />
  <DefaultLayoutOverride>
    <StartLayoutCollection>
      <defaultlayout:StartLayout GroupCellWidth="8"
xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayo
ut">
        <start:Group Name=""
xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout">
        <start:DesktopApplicationTile
```

```
            DesktopApplicationID="MSEdge"
            Size="2x2"
            Row="0"
            Column="0"/>
        <start:Tile
            AppUserModelID="Microsoft.Getstarted_8wekyb3d8bbwe!App"
            Size="4x2"
            Row="0"
            Column="2"/>
        <start:Tile

AppUserModelID="Microsoft.Office.PowerPoint_8wekyb3d8bbwe!Microsoft.pptim"
            Size="2x2"
            Row="2"
            Column="0"/>
        <start:Tile

AppUserModelID="Microsoft.Office.Word_8wekyb3d8bbwe!Microsoft.Word"
            Size="2x2"
            Row="2"
            Column="2"/>
        <start:Tile

AppUserModelID="Microsoft.Office.Excel_8wekyb3d8bbwe!Microsoft.Excel"
            Size="2x2"
            Row="2"
            Column="4"/>
        <start:Tile
            AppUserModelID="c5e2524a-ea46-4f67-841f-
6a9465d9d515_cw5n1h2txyewy!App"
            Size="2x2"
            Row="4"
            Column="0"/>
        <start:Tile
            AppUserModelID="microsoft.microsoftskydrive_8wekyb3d8bbwe!App"
            Size="2x2"
            Row="4"
            Column="2"/>
        <start:Tile

AppUserModelID="Microsoft.MicrosoftPowerBIForWindows_8wekyb3d8bbwe!Microsoft
.MicrosoftPowerBIForWindows"
            Size="2x2"
            Row="4"
            Column="4"/>
        <start:Tile
            AppUserModelID="signin.webex.com-8846C236_2aab1d9x9fqba!App"
            Size="2x2"
            Row="6"
            Column="0"/>
        <start:Tile
            AppUserModelID="zoom.us-F576B427_j0dtdqw38r40m!App"
            Size="2x2"
            Row="6"
            Column="2"/>
```

```
        <start:Tile
            AppUserModelID="www.youtube.com-756BE99A_pd8mbgmqs65xy!App"
            Size="2x2"
            Row="6"
            Column="4"/>
        </start:Group>
      </defaultlayout:StartLayout>
    </StartLayoutCollection>
  </DefaultLayoutOverride>
</LayoutModificationTemplate>
```

Appendix B: Extract AppUserModelIDs from installed apps

To obtain the AppUserModelID of apps installed on Surface Hub:

1. Sign in to Surface Hub as an admin, open **Settings**, and select **Update & Security**.
2. Select Logs. Insert a USB drive, then select **Collect logs.**
3. On a separate PC, open the USB drive and unzip the Log folder.
4. In the Registry folder, open **HKLM_SOFTWARE_Microsoft.txt**.
5. Search for the **ApplicationUserModelId** associated with the app you want to include in the Start menu.

```
102850 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel\StateRepository\Cache\ApplicationUser\Data\8c]
102851 "Application"=dword:0000006b
102852 "User"=dword:00000003
102853 "ApplicationUserModelId"="www.youtube.com-756BE99A_pd8mbgmqs65xy!App"
```

Related links

- Install Progressive Web Apps on Surface Hub

Manage Surface Hub settings

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

In this section

Topic	Description
Local management for Surface Hub settings	Learn about Surface Hub settings.
Accessibility	Accessibility settings for the Surface Hub can be changed by using the Settings app. You'll find them under Ease of Access. Your Surface Hub has most of the accessibility options in Windows 10 or Windows 11.
Change the Surface Hub device account	You can change the device account in Settings to either add an account if one was not already provisioned, or to change any properties of an account that was already provisioned.
Device reset	You may need to reset your Surface Hub.
Use fully qualified domain name with Surface Hub	Options to configure domain name with Surface Hub.
Wireless network management	Surface Hub offers two options for network connectivity to your corporate network and Internet: wireless, and wired. While both provide network access, we recommend you use a wired connection.

Local management for Surface Hub settings

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

After initial setup of Microsoft Surface Hub, the device's settings can be locally managed through **Settings**.

Surface Hub settings

Surface Hubs have many settings that are common to other Windows devices, but also have settings which are only configurable on Surface Hubs. This table lists settings only configurable on Surface Hubs.

Setting	Location	Description
Device account	Surface Hub > Accounts	Set or change the Surface Hub's device account.
Device account sync status	Surface Hub > Accounts	Check the sync status of the device account's mail and calendar on the Surface Hub.
Password rotation	Surface Hub > Accounts	Choose whether to let the Surface Hub automatically rotate the device account's password.
Change admin account password	Surface Hub > Accounts	Change the password for the local admin account. This is only available if you configured the device to use a local admin during first run.
Device Management	Surface Hub > Device management	Manage policies and business applications using mobile device management (MDM).
Provisioning packages	Surface Hub > Device management	Set or change provisioning packages installed on the Surface Hub.
Open the Microsoft Store app	Surface Hub > Apps & features	The Microsoft Store app is only available to admins through the Settings app.
Skype for Business domain name	Surface Hub > Calling & Audio	Configure a domain name for your Skype for Business server.
Default Speaker volume	Surface Hub > Calling & Audio	Configure the default speaker volume for the Surface Hub when it starts a session.

Setting	Location	Description
Default microphone and speaker settings	Surface Hub > Calling & Audio	Configure a default microphone and speaker for calls, and a default speaker for media playback.
Enable Dolby Audio X2	Surface Hub > Calling & Audio	Configure the Dolby Audio X2 speaker enhancements.
Open Connect App automatically	Surface Hub > Projection	Choose whether projection will automatically open the Connect app or wait for user input before opening.
Turn off wireless projection using Miracast	Surface Hub > Projection	Choose whether presenters can wirelessly project to the Surface Hub using Miracast.
Require a PIN for wireless projection	Surface Hub > Projection	Choose whether people are required to enter a PIN before they use wireless projection.
Wireless projection (Miracast) channel	Surface Hub > Projection	Set the channel for Miracast projection.
Meeting info shown on the welcome screen	Surface Hub > Welcome screen	Choose whether meeting organizer, time, and subject show up on the welcome screen.
Welcome screen background	Surface Hub > Welcome screen	Choose an image to be used as the background during user sessions and on the welcome screen.
Session timeout to Welcome screen	Surface Hub > Session & power	Choose how long until the Surface Hub returns to the welcome screen after no motion is detected.
Resume session	Surface Hub > Session & power	Choose to allow users to resume a session after no motion is detected or to automatically clean up a session.
Access to Microsoft 365 meetings and files	Surface Hub > Session & power	Choose whether a user can sign in to Microsoft 365 to get access to their meetings and files.

Setting	Location	Description
Turn on screen with motion sensors	Surface Hub > Session & power	Choose whether the screen turns on when motion is detected.
Screen time out	Surface Hub > Session & power	Choose how long the device needs to be inactive before turning off the screen.
Sleep time out	Surface Hub > Session & power	Choose how long the device needs to be inactive before going to sleep mode.
Friendly name	Surface Hub > About	Set the Surface Hub name that people will see when connecting wirelessly.
Maintenance hours	Update & security > Windows Update > Advanced options	Configure when updates can be installed.
Recover from the cloud	Update & security > Recovery	Reinstall the operating system on Surface Hub to a manufacturer build from the cloud.
Save BitLocker key	Update & security > Recovery	Back up your Surface Hub's BitLocker key to a USB drive.
Collect logs	Update & security > Logs	Save logs to a USB drive to send to Microsoft later.
Event viewer	Update & security > Logs	Launch Windows Event Viewer to see events that have happened on the Surface Hub.

Related topics

Manage Surface Hub settings

Remote Surface Hub management

Microsoft Surface Hub administrator's guide

Configure domain name for Skype for Business

Article • 01/19/2023

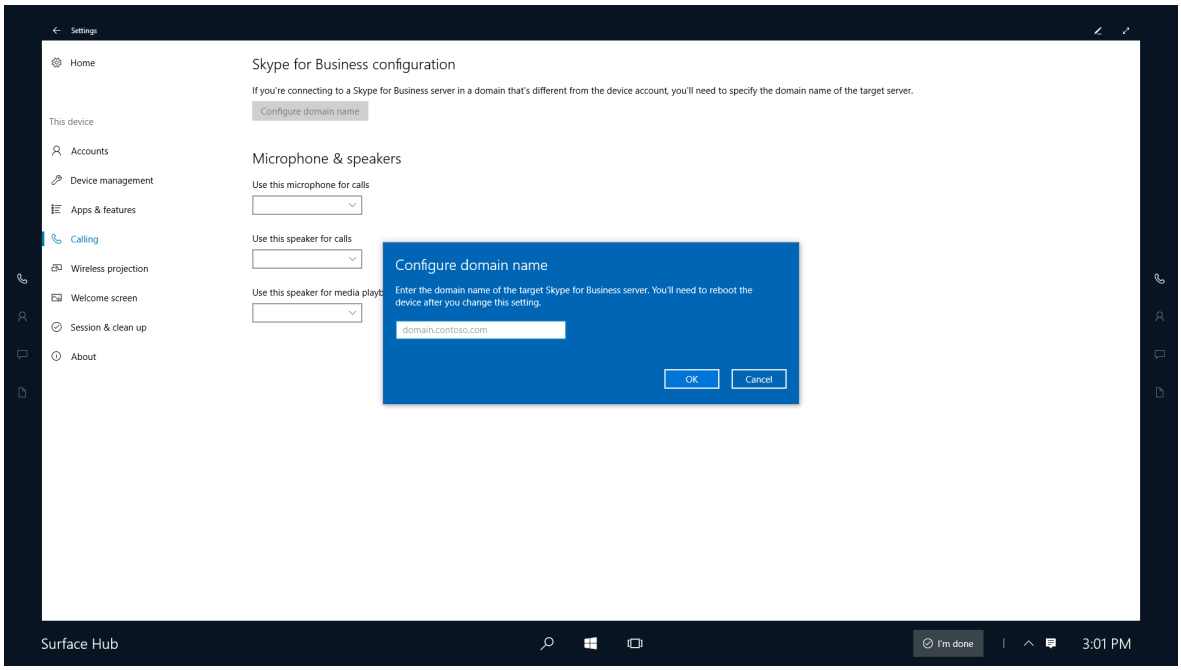
There are a few scenarios where you need to specify the domain name of your Skype for Business server:

- **Multiple DNS suffixes** - When your Skype for Business infrastructure has disjointed namespaces such that one or more servers have a DNS suffix that doesn't match the suffix of the sign-in address (SIP) for Skype for Business.
- **Skype for Business and Exchange suffixes are different** - When the suffix of the sign-in address for Skype for Business differs from the suffix of the Exchange address used for the device account.
- **Working with certificates** - Large organizations with on-premises Skype for Business servers commonly use certificates with their own root certificate authority (CA). It is common for the CA domain to be different than the domain of the Skype for Business server which causes the certificate to not be trusted, and sign-in fails. Skype needs to know the domain name of the certificate in order to set up a trust relationship. Enterprises typically use Group Policy to push this out to Skype desktop, but Group Policy is not supported on Surface Hub.

To configure the domain name for your Skype for Business server

1. On Surface Hub, open **Settings**.
2. Click **Surface Hub**, and then click **Calling & Audio**.
3. Under **Skype for Business configuration**, click **Configure domain name**.
4. Type the domain name for your Skype for Business server, and then click **Ok**.

> **Tip**
>
> You can type multiple domain names, separated by commas.
> For example: lync.com, outlook.com, lync.glbdns.microsoft.com


Settings
Home
This device
Accounts
Device management
Apps & features
Calling
Wireless projection
Welcome screen
Session & clean up
About
Skype for Business configuration
If you're connecting to a Skype for Business server in a domain that's different from the device account, you'll need to specify the domain name of the target server.
Configure domain name
Microphone & speakers
Use this microphone for calls
Use this speaker for calls
Use this speaker for media playb
Configure domain name
Enter the domain name of the target Skype for Business server. You'll need to reboot the device after you change this setting.
domain.contoso.com
OK
Cancel
Surface Hub
I'm done
3:01 PM

Wireless network management (Surface Hub)

Article • 01/03/2023

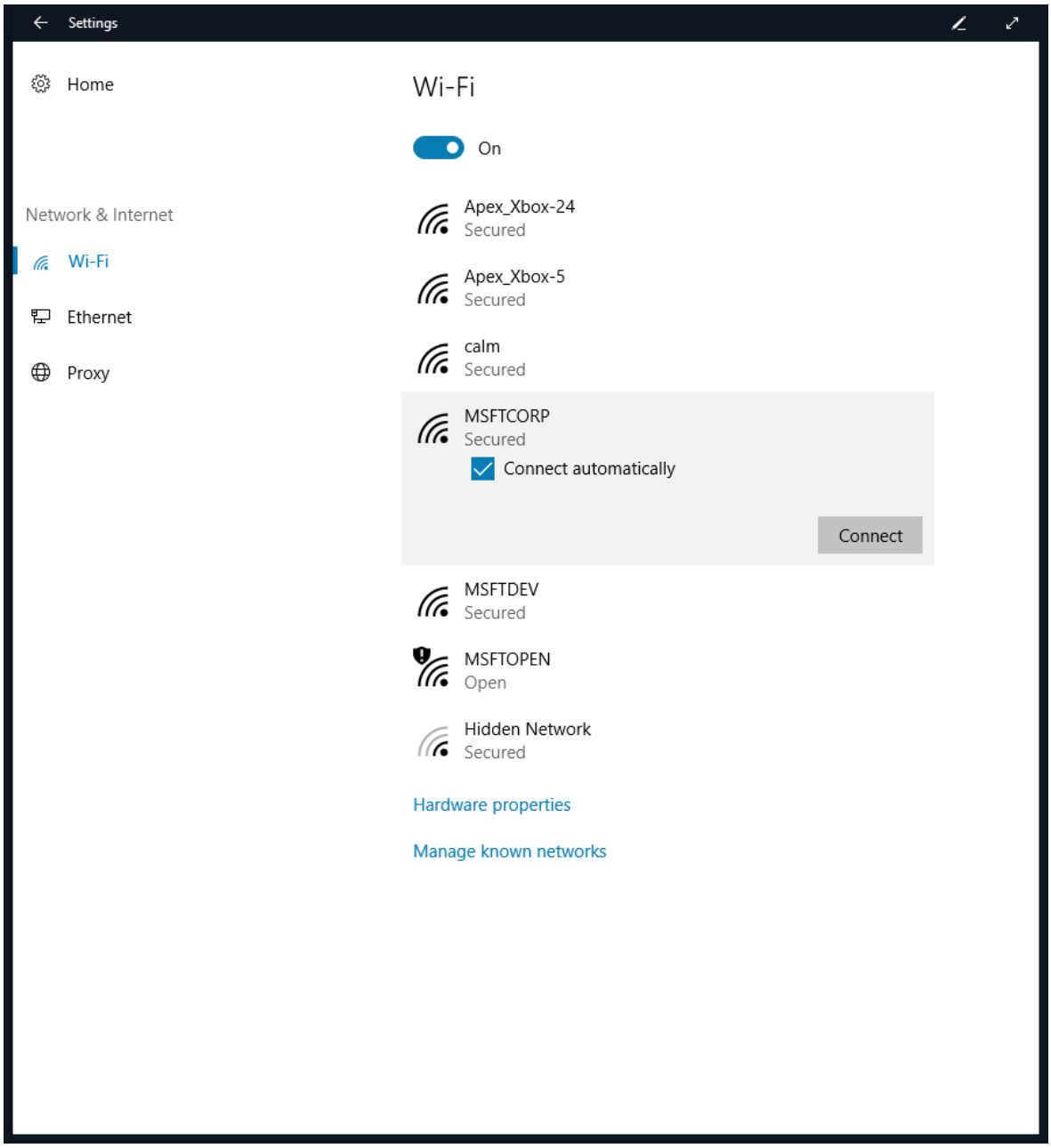
Microsoft Surface Hub offers two options for network connectivity to your corporate network and Internet: wireless, and wired. While both provide network access, we recommend you use a wired connection.

Modifying, adding, or reviewing a network connection

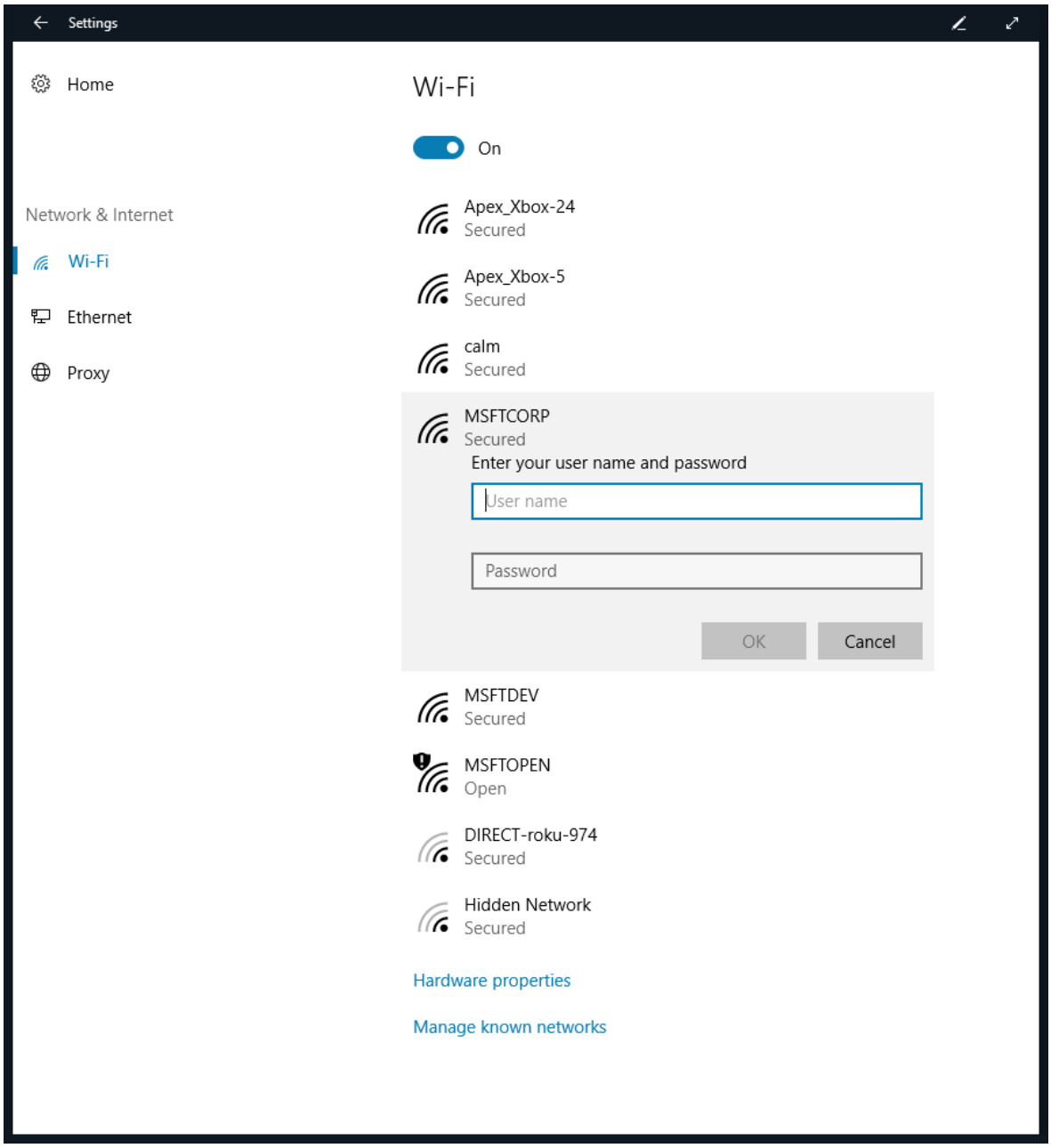
If a wired network connection is not available, the Surface Hub can use a wireless network for internet access. A properly connected and configured Wi-Fi access point must be available and within range of the Surface Hub.

Choose a wireless access point

1. On the Surface Hub, open **Settings** and enter your admin credentials.
2. Click **Network & Internet**. Under **Wi-Fi**, choose an access point. If you want Surface Hub to automatically connect to this access point, click **Connect automatically**. Click **Connect**.



3. If the network is secured, you'll be asked to enter the security key. Click **Next** to connect.



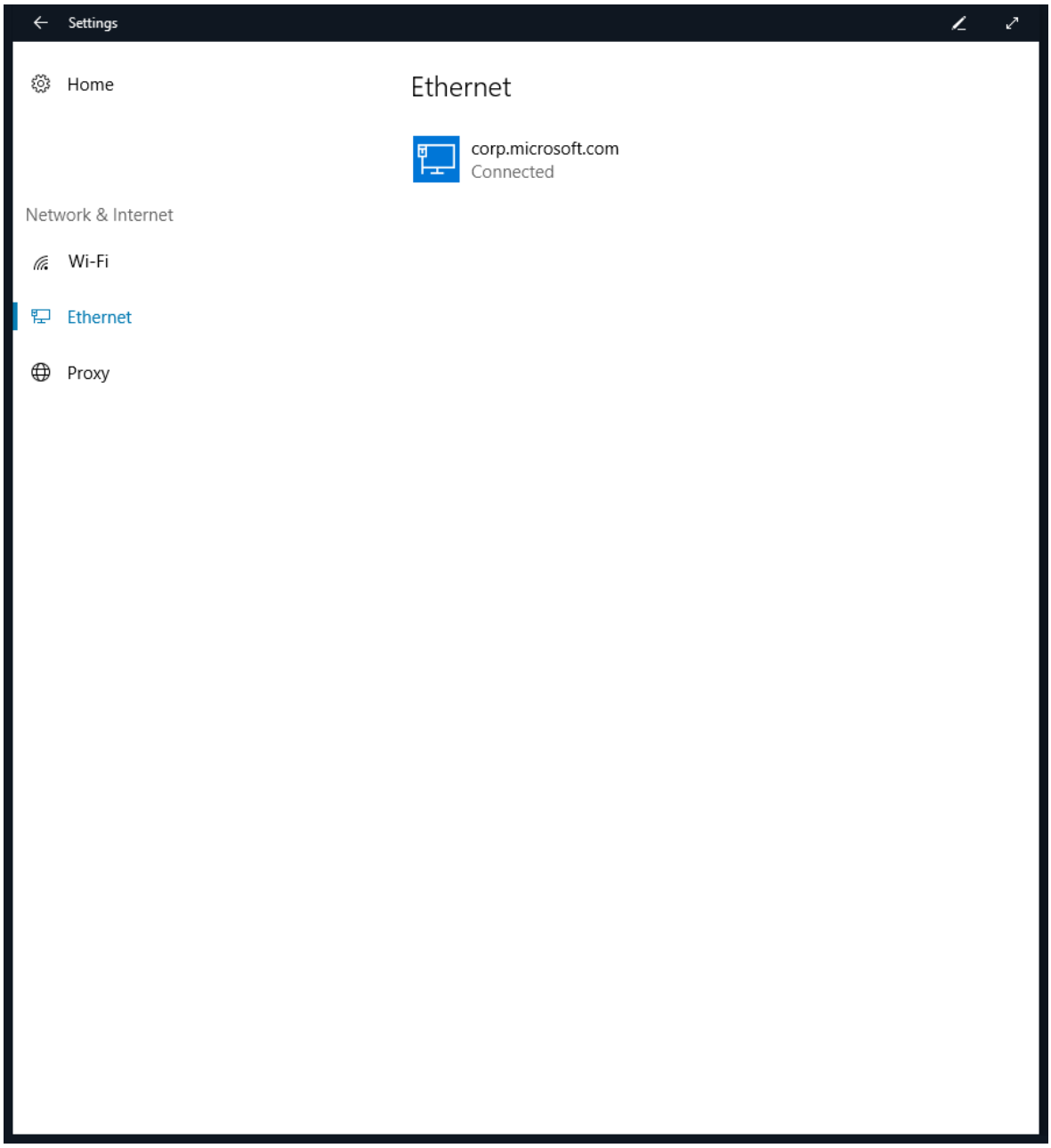
Review wireless settings

1. On the Surface Hub, open **Settings** and enter your admin credentials.
2. Click **Network & Internet**, then **Wi-Fi**, and then click **Advanced options**.
3. Surface Hub shows you the properties for the wireless network connection.

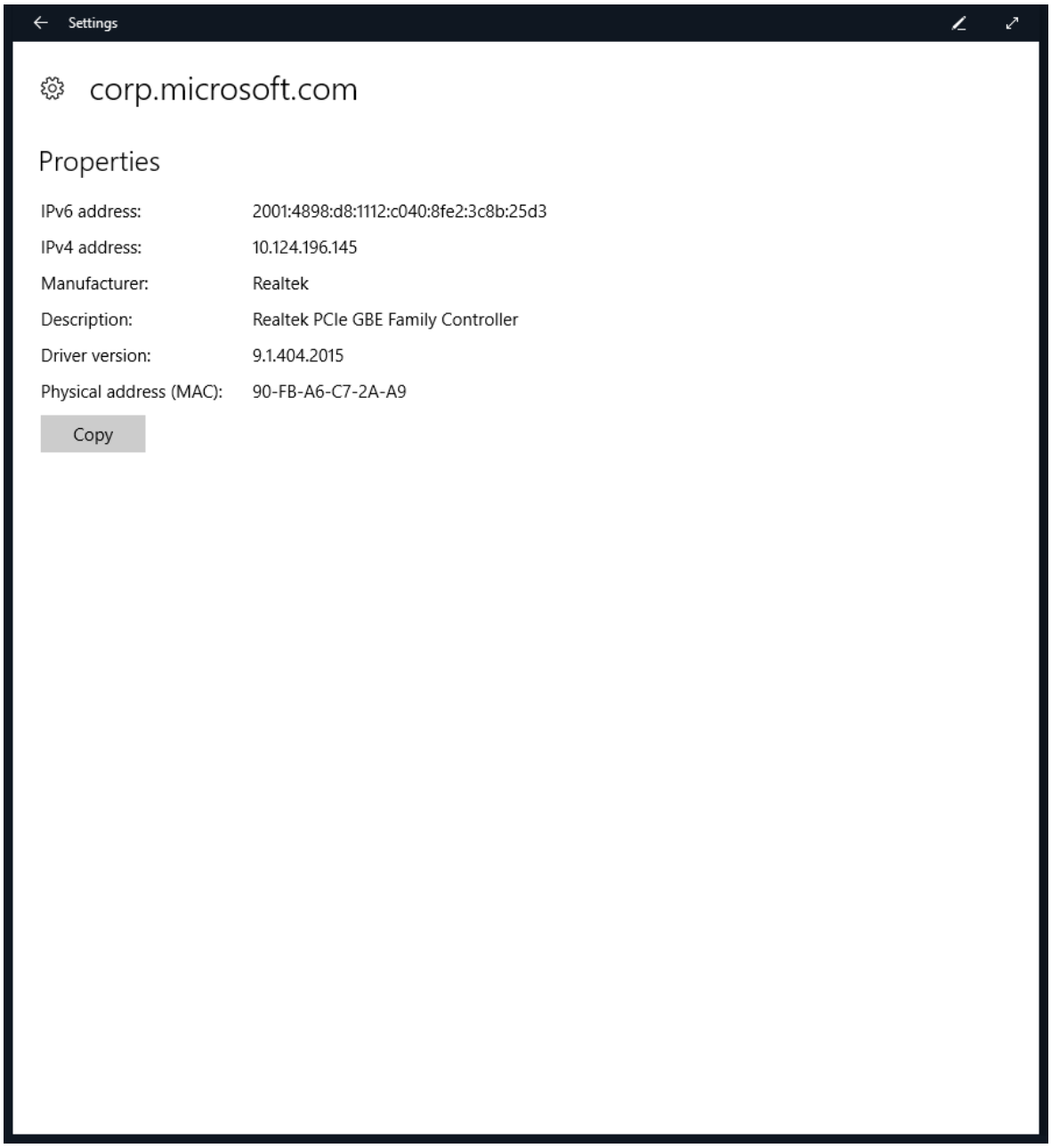
Review wired settings

1. On the Surface Hub, open **Settings** and enter your admin credentials.

2. Click **System**, click **Network & Internet**, then click on the network under Ethernet.



3. The system will show you the properties for the wired network connection.



Related topics

- Manage Microsoft Surface Hub
- Microsoft Surface Hub administrator's guide

Enable 802.1x wired authentication

Article • 03/16/2023 • Applies to: Surface Hub, Surface Hub 2S

The November 14, 2017 update to Windows 10 (build 15063.726) enabled 802.1x wired authentication policy configuration on Surface Hub devices. The feature allows organizations to enforce standardized wired network authentication using the IEEE 802.1x authentication protocol. This was already available for wireless authentication using WLAN profiles via MDM or provisioning package. This topic explains how to configure a Surface Hub for use with wired authentication.

Enforcement and enablement of 802.1x wired authentication on Surface Hub can be done through MDM OMA-URI profiles or provisioning package.

The primary configuration to set is the **LanProfile** policy. Depending on the authentication method selected, other policies may be required, either the **EapUserData** policy or through MDM policies for adding user or machine certificates (such as ClientCertificateInstall for user/device certificates or RootCATrustedCertificates for device certificates).

LanProfile policy element

To configure Surface Hub to use one of the supported 802.1x authentication methods, utilize the following OMA-URI.

```
./Vendor/MSFT/SurfaceHub/Dot3/LanProfile
```

This OMA-URI node takes a text string of XML as a parameter. The XML provided as a parameter should conform to the Wired LAN Profile Schema including elements from the 802.1X schema.

In most instances, an administrator or user can export the LanProfile XML from an existing PC that is already configured on the network for 802.1X using this following NETSH command.

```
netsh lan export profile folder=.
```

Running this command will give the following output and place a file titled **Ethernet.xml** in the current directory.

```
Interface: Ethernet
Profile File Name: .\Ethernet.xml
1 profile(s) were exported successfully.
```

To disable 802.1x completely on the Surface Hub, a provisioning package can be used to set the SurfaceHub\Dot3\LanProfile node to the following xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<LANProfile xmlns="https://www.microsoft.com/networking/LAN/profile/v1">
   <MSM>
       <security>
           <OneXEnforced>false</OneXEnforced>
           <OneXEnabled>false</OneXEnabled>
       </security>
  </MSM>
</LANProfile>
```

EapUserData policy element

If your selected authentication method requires a username and password as opposed to a certificate, you can use the **EapUserData** element to specify credentials for the device to use to authenticate to the network.

```
./Vendor/MSFT/SurfaceHub/Dot3/EapUserData
```

This OMA-URI node takes a text string of XML as a parameter. The XML provided as a parameter should conform to the PEAP MS-CHAPv2 User Properties example. In the example, you will need to replace all instances of *test* and *ias-domain* with your information.

Adding certificates

If your selected authentication method is certificate-based, you will need to create a provisioning package, utilize MDM, or import a certificate from settings (**Settings** >

Update and Security > **Certificates**) to deploy those certificates to your Surface Hub device in the appropriate Certificate Store. When adding certificates, each PFX must contain only one certificate (a PFX cannot have multiple certificates).

Surface Hub security overview

Article • 02/16/2023

Surface Hub provides a locked-down appliance-like experience with custom platform firmware running the Windows 10 Team operating system. The resulting device takes the traditional, "single-use" secure kiosk, "only run what you need" philosophy and delivers a modern take on it. Built to support a rich collaborative user experience, Surface Hub is protected against continually evolving security threats.

Built on Windows 10, Surface Hub delivers enterprise-grade modern security enabling IT admins to enforce data protection with BitLocker, Trusted Platform Module 2.0 (TPM), plus cloud-powered security with Windows Defender (also known as Microsoft Defender).

Defense-in-depth security

Security protocols begin as soon as Surface Hub is turned on. Starting at the firmware level, Surface Hub will only load the operating system and its components in response to multiple security checks. Surface Hub employs a Defense in Depth strategy that involves layering independent defensive sub-components to protect the whole of the system in the event of partial failure. This industry practice has proven to be highly effective in mitigating potential unilateral exploits and weaknesses in sub-components.

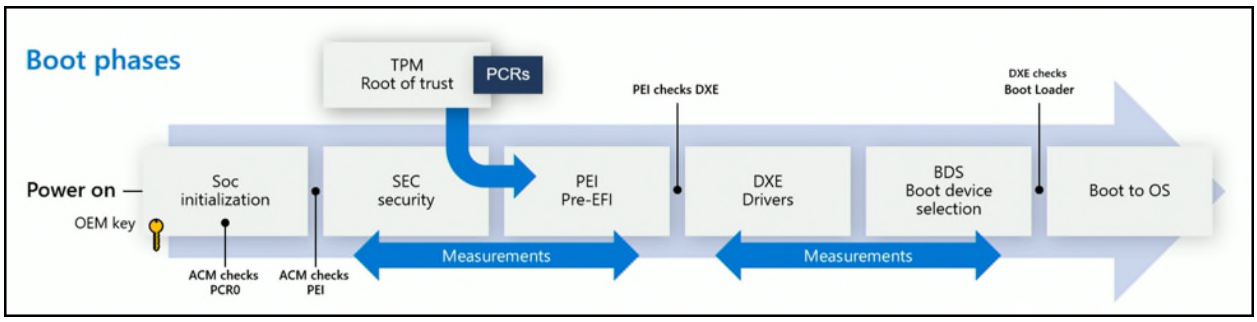
The modern Unified Extensible Firmware Interface (UEFI) is statically and securely configured by Microsoft to only boot an authenticated Windows 10 Team operating system from internal storage. Every line of code that runs on Surface Hub has its signature verified before execution. Only applications signed by Microsoft, either as part of the operating system or installed via the Microsoft Store, can run on the Surface Hub. Code or apps not meeting these requirements are blocked.

Surface Hub security systems include the following:

- **Boot-time defenses.** Loads only trusted Surface Hub operating system components.
- **Operating system defenses.** Protects against the execution of unintended or malicious software or code.
- **User interface defenses.** Provides a user interface that's safe for end users, preventing access to potentially risky activities such as running executables from the command line.

Boot-time defenses

The SoC has a security processor that's separate from every other core. When you first start Surface Hub, the security processor starts before anything else can be loaded.



Secure Boot

Secure Boot is used to verify that the components of the boot process, including drivers and the operating system, are validated against a database of valid and known signatures. On Surface Hub, a platform-specific signature must first be validated before the authorized Windows Team operating system can be loaded. This helps prevent attacks from a cloned or modified system running malicious code hidden in what appears to be an otherwise normal user experience. For more information, see Secure Boot overview.

Operating system defenses

Once the operating system is verified as originating from Microsoft and Surface Hub successfully completes the boot process, the device scrutinizes the executable code. Our approach to securing the operating system involves identifying the code signature of all executables, allowing only those that pass our restrictions to be loaded into the runtime. This code-signing method enables the operating system to verify the author and confirm that code was not altered prior to running on the device.

Surface Hub uses a code signing feature known as User Mode Code Integrity (UMCI) in Windows Application Control (formerly known as Device Guard). Policy settings are configured to only allow apps that meet one of these requirements:

- Universal Windows Platform (Microsoft Store) apps that are officially certified.
- Apps signed with the unique Microsoft Production Root Certification Authority (CA), which can only be signed by Microsoft employees with authorized access to those certificates.
- Apps signed with the unique Surface Hub Production Root C.

The configuration file is signed using the Microsoft Production Root CA designed to prevent restrictions from being removed or modified by a third party. All other executables at this point are simply blocked at the operating system runtime level and prevented from accessing processing power. This attack surface reduction provides the following protections:

- No legacy document modes
- No legacy script engines
- No Vector Markup Language
- No Browser Helper Objects
- No ActiveX controls

In addition to blocking unsigned or incorrectly signed code via UMCI, Surface Hub uses Windows Application Control to block Windows components, such as the Command Prompt, PowerShell, and Task Manager. These safeguards reflect a key design feature of Surface Hub as a secure computing appliance. For more information, see the following:

- Application Control overview
- Windows Defender Application Control and virtualization-based protection of code integrity

User interface defenses

While boot-time defenses and operating system lockdown safeguards deliver foundational security, the user interface provides an additional layer designed to further reduce risk. To prevent malicious code from reaching the device through drivers, Surface Hub does not download advanced drivers for plug and play (PnP) devices. Devices that leverage basic drivers, such as USB flash drives or certified Surface Hub peripherals (speakers, microphones, cameras), work as expected, but advanced systems, such as printers, will not.

User interface defenses also simplify the UI, further preventing the execution of malicious software or code. The following Surface Hub UI elements layer the core security provided by code signing:

- **File Explorer.** Surface Hub has a custom File Explorer that enables quick access to Music, Videos, Documents, Pictures, and Downloads folders — without exposing users to system or program files. Other locations on the local hard drive are not available through File Explorer. In addition, many file types running, such as .exe and .msi installation files, cannot run, providing another layer of safety against potentially malicious executables.

- **Start & All Apps.** The Start and All Apps components of Surface Hub do not expose access to Command Prompt, PowerShell, or other Windows components blocked via Application Control. In addition, Windows run functionality typically accessed on PCs from the Search box is turned off for Surface Hub.

Security enhancements in Surface Hub 2S

Although Surface Hub and Surface Hub 2S both run the same operating system software, some features unique to Surface Hub 2S provide additional management and security capabilities, enabling IT admins to perform the following tasks:

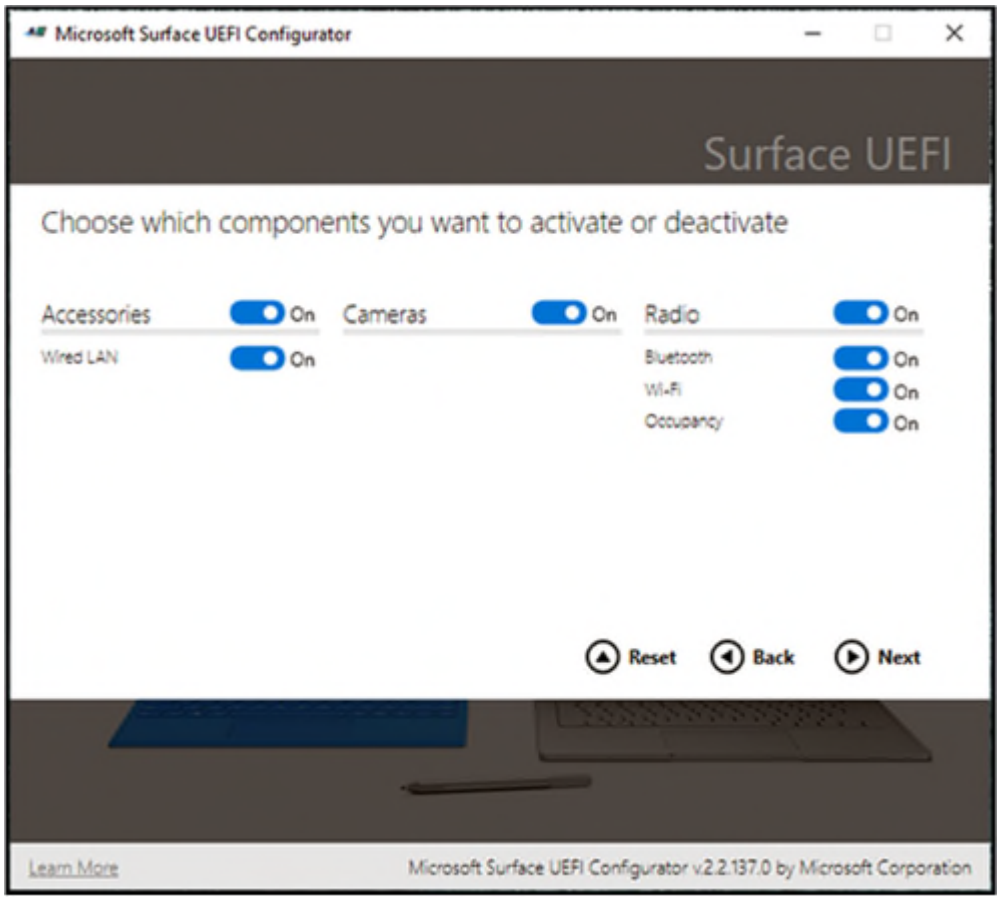
- Manage UEFI settings with SEMM
- Recover Hub with bootable USB
- Harden device account with password rotation

Manage UEFI settings with SEMM

UEFI is an interface between the underlying hardware platform pieces and the operating system. On Surface Hub, a custom UEFI implementation allows granular control over these settings and prevents any non-Microsoft entity from changing the UEFI settings of the device — or booting to a removable drive to modify or change the operating system.

At a high level, during the factory provisioning process, Surface Hub UEFI is preconfigured to enable Secure Boot and is set to only boot from the internal solid-state drive (SSD), with access to UEFI menus locked down and shortcuts removed. This seals UEFI access and ensures the device can only boot into the Windows Team operating system installed on Surface Hub.

When managed via Microsoft Surface Enterprise Management Mode (SEMM), IT admins can deploy UEFI settings on Hub devices across an organization. This includes the ability to enable or disable built-in hardware components, protect UEFI settings from being changed by unauthorized users, and adjust boot settings.



Admins can implement SEMM and enrolled Surface Hub 2S devices using the downloadable Microsoft Surface UEFI Configurator. For more information, see Secure and manage Surface Hub 2S with SEMM and UEFI. Secured using a certificate to protect the configuration from unauthorized tampering or removal, SEMM enables management of the following components:

- Wired LAN
- Camera
- Bluetooth
- Wi-Fi
- Occupancy sensor
- IPv6 for PXE Boot
- Alternate Boot
- Boot Order Lock
- USB Boot
- UEFI front page interface
  - Devices
  - Boot
  - Date/Time

Recover Hub with bootable USB

Surface Hub 2S enables admins to reinstall the device to factory settings using a recovery image in as little as 20 minutes. Typically, you would only need to do this if your Surface Hub is no longer functioning. Recovery is also useful if you have lost the Bitlocker key or no longer have admin credentials to the Settings app.

Harden device account with password rotation

Surface Hub uses a device account, also known as a "room account," to authenticate with Exchange, Microsoft Teams, and other services. When you enable password rotation, Hub 2S automatically generates a new password every seven days, consisting of 15-32 characters with a combination of uppercase and lowercase letters, numbers, and special characters. Because no one knows the password, the device account password rotation effectively mitigates associated risks from human error and potential social engineering security attacks.

Enterprise-grade security

In addition to Surface Hub-specific configurations and features addressed in this document, Surface Hub also uses standard Windows security features. These include:

- **BitLocker**. The Surface Hub SSD is equipped with BitLocker to protect the data on the device. Its configuration follows industry standards. For more information, see BitLocker overview.
- **Windows Defender.** The Windows Defender anti-malware engine runs continuously on Surface Hub and works to automatically remediate threats found on Surface Hub. The Windows Defender engine receives updates automatically and is manageable via remote management tools for IT admins. The Windows Defender engine is a perfect example of our Defense in Depth approach: If malware can find a way around our core code-signage-based security solution, it will be caught here. For more information, see Windows Defender Application Control and virtualization-based protection of code integrity.
- **Plug and play drivers.** To prevent malicious code from reaching the device through drivers, Surface Hub does not download advanced drivers for PnP devices. This allows devices that leverage basic drivers such as USB flash drives to work as expected while blocking more advanced systems such as printers.
- **Trusted Platform Module 2.0.** Surface Hub has an industry standard discrete Trusted Platform Module (dTPM) for generating and storing cryptographic keys and hashes. The dTPM protects keys used for the verification of boot phases, the BitLocker master key, password-less sign-on key, and more. The dTPM meets FIPS

140-2 Level 2 certification, the U.S. government computer security standard, and is compliant with Common Criteria certification used worldwide.

Wireless security for Surface Hub

Surface Hub uses Wi-Fi Direct / Miracast technology and the associated 802.11, Wi-Fi Protected Access (WPA2), and Wireless Protected Setup (WPS) standards. Since the device only supports WPS (as opposed to WPA2 Pre-Shared Key (PSK) or WPA2 Enterprise), issues traditionally associated with 802.11 encryption are simplified by design.

Surface Hub operates on par with the field of Miracast receivers. So, it's vulnerable to a similar set of exploits as all WPS-based wireless network devices. But the Surface Hub implementation of WPS has extra precautions built in. Also, its internal architecture helps prevent an attacker who has compromised the Wi-Fi Direct/Miracast layer from moving past the network interface onto other attack surfaces and connected enterprise networks.

Miracast is part of the Wi-Fi Display standard, which itself is supported by the Wi-Fi Direct protocol. These standards are supported in modern mobile devices for screen sharing and collaboration. Wi-Fi Direct or Wi-Fi "peer to peer" (P2P) is a standard released by the Wi-Fi Alliance for "Ad-Hoc" networks. This allows supported devices to communicate directly and create groups of networks without requiring a traditional Wi-Fi Access Point or an Internet connection.

Security for Wi-Fi Direct is provided by WPA2 using the WPS standard. Devices can be authenticated using a numerical pin, a physical or virtual push button, or an out-of-band message using near-field communication. Surface Hub supports both push button by default as well PIN methods.

How Surface Hub addresses Wi-Fi Direct vulnerabilities

Vulnerabilities and attacks in the Wi-Fi Direct invitation, broadcast, and discovery process: Wi-Fi Direct/Miracast attacks may target weaknesses in the group establishment, peer discovery, device broadcast, or invitation processes.

Wi-Fi Direct vulnerability	Surface Hub mitigation

Wi-Fi Direct vulnerability	Surface Hub mitigation
The discovery process may remain active for an extended period of time, which could allow invitations and connections to be established without the approval of the device owner.	Surface Hub only operates as the group owner, which doesn't perform the client discovery or GO negotiation processes. You can fully disable wireless projection to turn off broadcast.
Invitation and discovery through PBC allow an unauthenticated attacker to perform repeated connection attempts, or unauthenticated connections are automatically accepted.	By requiring WPS PIN security, administrators can reduce the potential for such unauthorized connections or "invitation bombs," in which invitations are repeatedly sent until a user mistakenly accepts one.

Wi-Fi Protected Setup (WPS) push button connect (PBC) vs PIN entry: Public weaknesses have been demonstrated in WPS-PIN method design and implementation. WPS-PBC has other vulnerabilities that could allow active attacks against a protocol that's designed for one-time use.

Wi-Fi Direct vulnerability	Surface Hub mitigation
WPS-PBC is vulnerable to active attackers. The WPS specification states: "*The PBC method has zero bits of entropy and only protects against passive eavesdropping attacks. PBC protects against eavesdropping attacks and takes measures to prevent a device from joining a network that was not selected by the device owner. The absence of authentication, however, means that PBC does not protect against active attack.*" Attackers can use selective wireless jamming or other denial-of-service techniques to trigger an unintended Wi-Fi Direct GO or connection. Also, an active attacker who merely has physical proximity can repeatedly tear down any Wi-Fi Direct group and attempt the attack until it succeeds.	Enable WPS-PIN security in Surface Hub configuration. The Wi-Fi WPS specification states: "The PBC method should only be used if no PIN-capable registrar is available and the WLAN user is willing to accept the risks associated with PBC."
WPS-PIN implementations can be subject to brute-force attacks that target a vulnerability in the WPS standard. The design of split PIN verification led to multiple implementation vulnerabilities over the past several years across a range of Wi-Fi hardware manufacturers. In 2011, researchers Stefan Viehböck and Craig Heffner released information about this vulnerability and tools such as "Reaver" as a proof of concept.	The Microsoft implementation of WPS in Surface Hub changes the PIN every 30 seconds. To crack the PIN, an attacker must complete the entire exploit in less than 30 seconds. Given the current state of tools and research in this area, a brute-force PIN-cracking attack through WPS is unlikely to succeed.

Wi-Fi Direct vulnerability	Surface Hub mitigation
WPS-PIN can be cracked by an offline attack because of weak initial key (E-S1, E-S2) entropy. In 2014, Dominique Bongard described a "Pixie Dust" attack where poor initial randomness for the pseudorandom number generator (PRNG) in the wireless device allowed an offline brute-force attack.	The Microsoft implementation of WPS in Surface Hub is not susceptible to this offline PIN brute-force attack. The WPS-PIN is randomized for each connection.

Unintended exposure of network services: Network daemons that are intended for Ethernet or WLAN services may be accidentally exposed because of misconfiguration (such as binding to "all"/0.0.0.0 interfaces). Other possible causes include a poorly configured device firewall or missing firewall rules.

Wi-Fi Direct vulnerability	Surface Hub mitigation
Misconfiguration binds a vulnerable or unauthenticated network service to "all" interfaces, which includes the Wi-Fi Direct interface. This can expose services that shouldn't be accessible to Wi-Fi Direct clients, which may be weakly or automatically authenticated.	In Surface Hub, the default firewall rules only permit the required TCP and UDP network ports and, by default, deny all inbound connections. Configure strong authentication by enabling the WPS-PIN mode.

Bridging Wi-Fi Direct and other wired or wireless networks: Network bridging between WLAN or Ethernet networks is a violation of the Wi-Fi Direct specification. Such a bridge or misconfiguration may effectively lower or remove wireless access controls for the internal corporate network.

Wi-Fi Direct vulnerability	Surface Hub mitigation
Wi-Fi Direct devices could allow unauthenticated or poorly authenticated access to bridged network connections. This might allow Wi-Fi Direct networks to route traffic to internal Ethernet LAN or other infrastructure or to enterprise WLAN networks in violation of existing IT security protocols.	Surface Hub can't be configured to bridge wireless interfaces or allow routing between disparate networks. The default firewall rules add defense in depth to any such routing or bridge connections.

The use of Wi-Fi Direct "legacy" mode: Exposure to unintended networks or devices may occur when you operate in "legacy" mode. Device spoofing or unintended connections could occur if WPS-PIN is not enabled.

Wi-Fi Direct vulnerability	Surface Hub mitigation

Wi-Fi Direct vulnerability	Surface Hub mitigation
By supporting both Wi-Fi Direct and 802.11 infrastructure clients, the system is operating in a "legacy" support mode. This may expose the connection-setup phase indefinitely, allowing groups to be joined or devices invited to connect well after their intended setup phase terminates.	Surface Hub doesn't support Wi-Fi Direct legacy clients. Only Wi-Fi Direct connections can be made to Surface Hub even when WPS-PIN mode is enabled.

Wi-Fi Direct GO negotiation during connection setup: The group owner in Wi-Fi Direct is analogous to the "access point" in a conventional 802.11 wireless network. The negotiation can be gamed by a malicious device.

Wi-Fi Direct vulnerability	Surface Hub mitigation
If groups are dynamically established, or the Wi-Fi Direct device can be made to join new groups, the group owner negotiation can be won by a malicious device that always specifies the maximum group owner "intent" value of 15. (But the connection fails if the device is configured to always be a group owner.)	Surface Hub takes advantage of Wi-Fi Direct "Autonomous mode," which skips the GO negotiation phase of connection setup. And Surface Hub is always the group owner.

Unintended or malicious Wi-Fi deauthentication: Wi-Fi deauthentication is an old attack in which a local attacker can expedite information leaks in the connection-setup process, trigger new four-way handshakes, target Wi-Fi Direct WPS-PBC for active attacks, or create denial-of-service attacks.

Wi-Fi Direct vulnerability	Surface Hub mitigation
Deauthentication packets can be sent by an unauthenticated attacker to cause the station to re-authenticate and then sniff the resulting handshake. Cryptographic or brute-force attacks can be attempted on the resulting handshake. Mitigation for these attacks includes enforcing length and complexity policies for pre-shared keys, configuring the access point (if applicable) to detect malicious levels of deauthentication packets, and using WPS to automatically generate strong keys. In PBC mode, the user interacts with a physical or virtual button to allow arbitrary device association. This process should happen only at setup, within a short window. After the button is automatically "pushed," the device will accept any station that associates via a canonical PIN value (all zeros). Deauthentication can force a repeated setup process.	Surface Hub uses WPS in PIN or PBC mode. No PSK configuration is permitted. This method helps enforce generation of strong keys. It's best to enable WPS-PIN security for Surface Hub.

Wi-Fi Direct vulnerability	Surface Hub mitigation
In addition to denial-of-service attacks, deauthentication packets can be used to trigger a reconnect that re-opens the window of opportunity for active attacks against WPS-PBC.	Enable WPS-PIN security in the Surface Hub configuration.

Basic wireless information disclosure: Wireless networks, 802.11 or otherwise, are inherently at risk of information disclosure. Although this information is mostly connection or device metadata, this problem remains a known risk for any 802.11 network administrator. Wi-Fi Direct with device authentication via WPS-PIN effectively reveals the same information as a PSK or Enterprise 802.11 network.

Wi-Fi Direct vulnerability	Surface Hub mitigation
During broadcast, connection setup, or even normal operation of already-encrypted connections, basic information about devices and packet sizes is wirelessly transmitted. At a basic level, a local attacker who's within wireless range can examine the relevant 802.11 information elements to determine the names of wireless devices, the MAC addresses of communicating equipment, and possibly other details, such as the version of the wireless stack, packet sizes, or the configured access point or group owner options.	The Wi-Fi Direct network that Surface Hub uses can't be further protected from metadata leaks, just like for 802.11 Enterprise or PSK wireless networks. Physical security and removal of potential threats from wireless proximity can help reduce potential information leaks.

Wireless evil twin or spoofing attacks: Spoofing the wireless name is a simple, well-known exploit a local attacker can use to lure unsuspecting or mistaken users to connect.

Wi-Fi Direct vulnerability	Surface Hub mitigation
By spoofing or cloning the wireless name or "SSID" of the target network, an attacker may trick the user into connecting to a fake, malicious network. By supporting unauthenticated, auto-join Miracast, an attacker could capture the intended display materials or launch network attacks on the connecting device.	While there are no specific protections against joining a spoofed Surface Hub, this vulnerability is partially mitigated in two ways. First, any potential attack must be physically within Wi-Fi range. Second, this attack is only possible during the first connection. Subsequent connections use a persistent Wi-Fi Direct group, and Windows will remember and prioritize this prior connection during future Hub use. (Note: Spoofing the MAC address, Wi-Fi channel, and SSID simultaneously was not considered for this report and may result in inconsistent Wi-Fi behavior.) Overall, this weakness is a fundamental problem for any 802.11 wireless network that lacks Enterprise WPA2 protocols such as EAP-TLS or EAP-PWD, which Wi-Fi Direct doesn't support.

Surface Hub hardening guidelines

Surface Hub is designed to facilitate collaboration and allow users to start or join meetings quickly and efficiently. The default Wi-Fi Direct settings for Surface Hub are optimized for this scenario.

For additional wireless interface security, Surface Hub users should enable the WPS-PIN security setting. This setting disables WPS-PBC mode and offers client authentication. It provides the strongest level of protection by preventing unauthorized connection to Surface Hub.

If you still have concerns about authentication and authorization for Surface Hub, we recommend that you connect the device to a separate network. You could use Wi-Fi (such as a "guest" Wi-Fi network) or a separate Ethernet network, preferably an entirely different physical network. But a VLAN can also provide added security. Of course, this approach may preclude connections to internal network resources or services and may require additional network configuration to regain access.

Also recommended:

- Install regular system updates
- Update Miracast settings to disable auto-present mode

Learn more

- Secure Boot overview
- BitLocker overview
- Application Control overview
- Secure and manage Surface Hub 2S with SEMM and UEFI
- How Surface Hub addresses Wi-Fi Direct security issues
- Windows Defender Application Control and virtualization-based protection of code integrity
- Surface Tools for IT
- FIPS 140-2 Level 2
- Common Criteria certification

Password management (Surface Hub)

Article • 04/14/2023 • Applies to: Surface Hub, Surface Hub 2S

Every Microsoft Surface Hub device account requires a password to authenticate and enable features on the device. For security reasons, you may want to change (or "rotate") this password regularly. However, if the device account's password changes, the password that was previously stored on the Surface Hub will be invalid, and all features that depend on the device account will be disabled. You will need to update the device account's password on the Surface Hub from the Settings app to re-enable these features.

To simplify password management for your Surface Hub device accounts, there are two options:

1. Turn off password expiration for the device account.
2. Allow the Surface Hub to automatically rotate the device account's password.

Turn off password rotation for the device account

Set the device account's **PasswordNeverExpires** property to True. You should verify whether this meets your organization's security requirements.

Allow the Surface Hub to automatically rotate the device account's password

The Surface Hub can automatically change a device account's password without requiring you to manually update it. You can enable this feature in **Settings** > **Surface Hub** > **Accounts**. If you turn on Password Rotation, the Surface Hub will attempt to change the password every 7 days during maintenance hours. Passwords do not change during a meeting. If 7 days have passed since the last password rotation, but the Surface Hub was off, it will attempt to change the password immediately when turned on or every 10 minutes until successful.

The automatically generated passwords contain 15-32 characters including a combination of uppercase and lowercase letters, numbers, and special characters. Note that when the device account's password is changed, you will not be shown the new password. If you need to sign in to the account, or to provide the password again (for example, if you want to change the device account settings on the Surface Hub), then

you'll need use Active Directory or the Microsoft 365 admin portal to reset the password.

> **ⓘ Important**
>
> The **device affiliation** option selected during initial setup of the Surface Hub has an impact on which device account format can be used with password rotation. Hubs affiliated with an on-premise Active Directory can only rotate passwords of device accounts entered in **domain\username** format. Hubs affiliated with an Azure Active Directory can only rotate passwords of device accounts entered in `username@domain.com` format, but only if the account is cloud-only or if the AAD domain is configured for **cloud authentication** and **password writeback**.

Configure passwordless sign-in on Surface Hub

Article • 04/14/2023

When you sign in to Surface Hub, you'll see all your meetings and all your recent Microsoft 365 files. You can open your presentation, document, whiteboard, or workbook without having to project from a PC or send the file.

Passwordless sign-in simplifies access to your apps, meetings, and files. Surface Hub supports signing in using the Microsoft Authenticator app and FIDO2 security keys provided by your organization.

Organization prerequisites

To let people in your organization sign in to Surface Hub with their phones and other devices instead of a password, you'll need to make sure that your organization meets these prerequisites:

- Your organization must be a hybrid or cloud-only organization, backed by Azure Active Directory (Azure AD). For more information, see What is Azure Active Directory?
- Make sure you have at minimum a Microsoft 365 E3 subscription.
- Configure Multi-Factor Authentication. Make sure **Notification through mobile app** is selected.
- Enable content hosting on Azure AD services such as Office, SharePoint, etc.
- Surface Hub must be running Windows 10, version 1703 or later.
- Surface Hub is set up with either a local or domain-joined account.

To learn more see:

- Enable passwordless phone sign-in
- Enable passwordless security key sign-in

Configure sign-in using Microsoft Authenticator app

Starting with the Windows 10 Team 2020 Update, you can sign in with your preferred email alias in Azure AD or your User Principal Name (UPN) to sign in with Microsoft Authenticator. For example:

- Preferred alias format: sofia.gomes@contoso.com
- UPN format: sgomes@contoso.com

The Microsoft Authenticator app helps you sign-in to Surface Hub using your mobile device. To configure sign-in using Microsoft Authenticator:

1. On your mobile device, download the Microsoft Authenticator app.
    - Google Android: On your Android device, go to Google Play to download and install the Microsoft Authenticator app.
    - Apple iOS: On your Apple iOS device, go to the App Store to download and install the Microsoft Authenticator app.
2. On your PC, setup the Microsoft Authenticator app from the Security info page for your work or school account.
3. From the Microsoft Authenticator app on your mobile device, turn on and use phone sign-in for your work or school account.

Configure sign-in using FIDO2 security keys

> **Note**
>
> Passwordless sign-in on Surface Hub using FIDO2 security keys requires the **Windows 10 Team 2020 Update**.

> **Important**
>
> Surface Hub only supports USB security keys.

You can also sign into Surface Hub using a FIDO2 security key provided by your organization.

To configure sign-in using a security key

1. On your PC, go to your https://myprofile.microsoft.com/ page and sign in to your work or school account.
2. Select **Security info** > **Add sign-in method**.

3. Select **Security key** from the drop-down list, and then select **Add**.
4. On the **Security key** page, choose **USB device**.
5. Have your security key ready and select **Next**. In the dialog box that appears, follow the instructions to insert the security key, create or enter a PIN, and perform the required gesture (either biometric or touch).
6. On the **Security key** page, give your security key a name, then select **Next**. Select **Done** to complete the process.

Sign in to Surface Hub

Once you've configured passwordless sign-in, you can use it to make it easier to access your apps, meetings, and files on the Surface Hub.

Sign in during a meeting

1. After you've set up a meeting, go to the Surface Hub and select **Sign in to see your meetings and files**.
2. You'll see a list of the people invited to the meeting. Select yourself (or the person who wants to sign in – make sure this person has gone through the steps to set up their device before your meeting), and then select **Continue**. You'll see a code on the Surface Hub.
3. To approve the sign-in, open the Authenticator app, enter the four-digit code that's displayed on the Surface Hub, and select **Approve**. You will then be asked to enter the PIN or use your fingerprint to complete the sign in. You can now access all files through the OneDrive app.

Sign in to apps

- Quickly sign in to Microsoft apps like Whiteboard, PowerPoint, Word, Excel, OneDrive, and Power BI.
- Once you've signed into Surface Hub, you can use other apps without having to sign in again until you select **End session**. Selecting **End session** deletes your credentials, files, and personal data from the device. For more information, see End session.

Learn more

- Passwordless authentication options for Azure Active Directory
- Passwordless sign-in with the Microsoft Authenticator app
- Passwordless sign-in using FIDO2 security keys

Secure and manage Surface Hub 2S with SEMM and UEFI

Article • 01/03/2023

New in Surface Hub 2S, you can use SEMM to manage the UEFI setting of the device. Use the Microsoft Surface UEFI Configurator to control the following components:

- Wired LAN
- Cameras
- Bluetooth
- Wi-Fi
- Occupancy sensor

Use the Microsoft Surface UEFI Configurator to turn on or off the following UEFI settings:

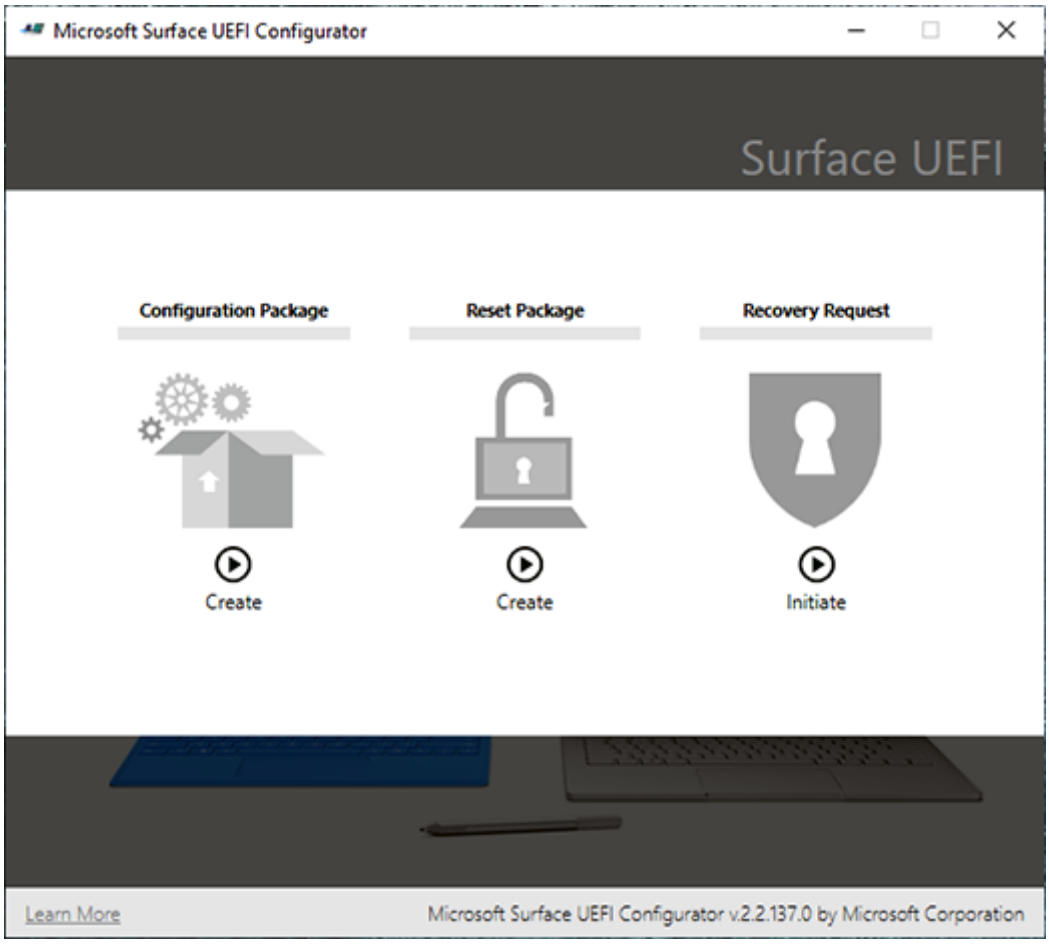
- Boot
  - IPv6 for PXE Boot
  - Alternate Boot
  - Boot Order Lock
  - USB Boot
- UEFI Front Page
  - Devices
  - Boot
  - Date/Time

Create UEFI configuration image

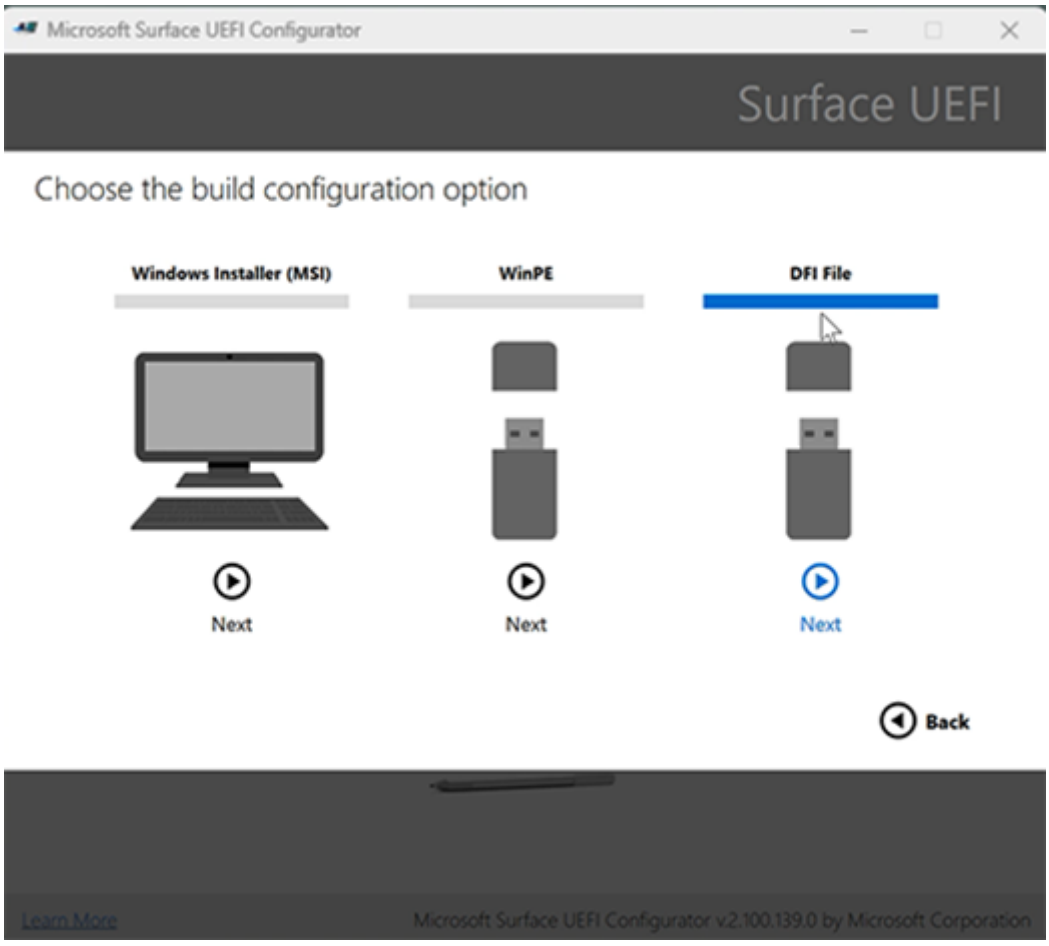
Unlike other Surface devices, you cannot use an MSI file or a Win PE image to apply these settings on Surface Hub 2S. Instead, you need to create a USB image to load into the device. To create a Surface Hub 2S UEFI configuration image, download and install the latest version of the Microsoft Surface UEFI Configurator from the Surface Tools for IT page in the Microsoft Download Center. For more information about using UEFI and SEMM, see Microsoft Surface Enterprise Management Mode.

To configure UEFI on Surface Hub 2S

1. Start the UEFI Configurator and on the first screen, choose **Configuration Package**.

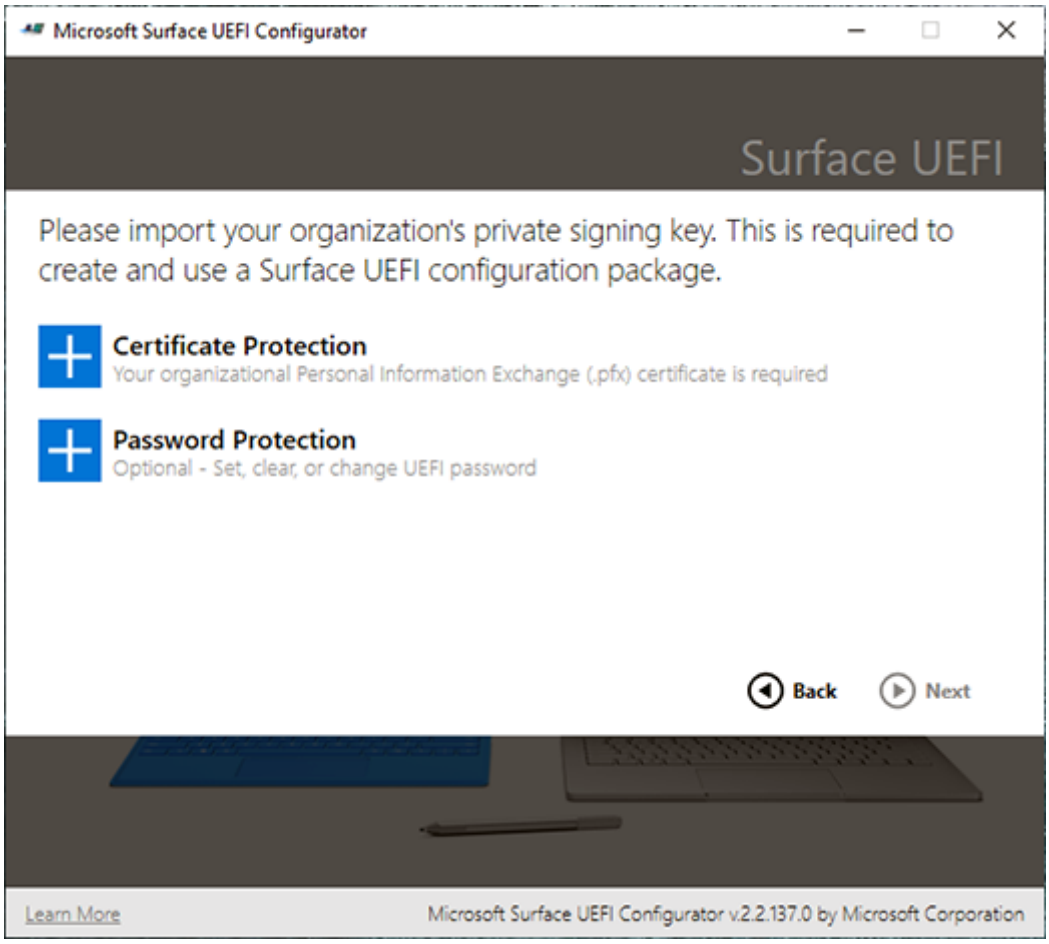


2. Select **DFI File** as the build configuration option.

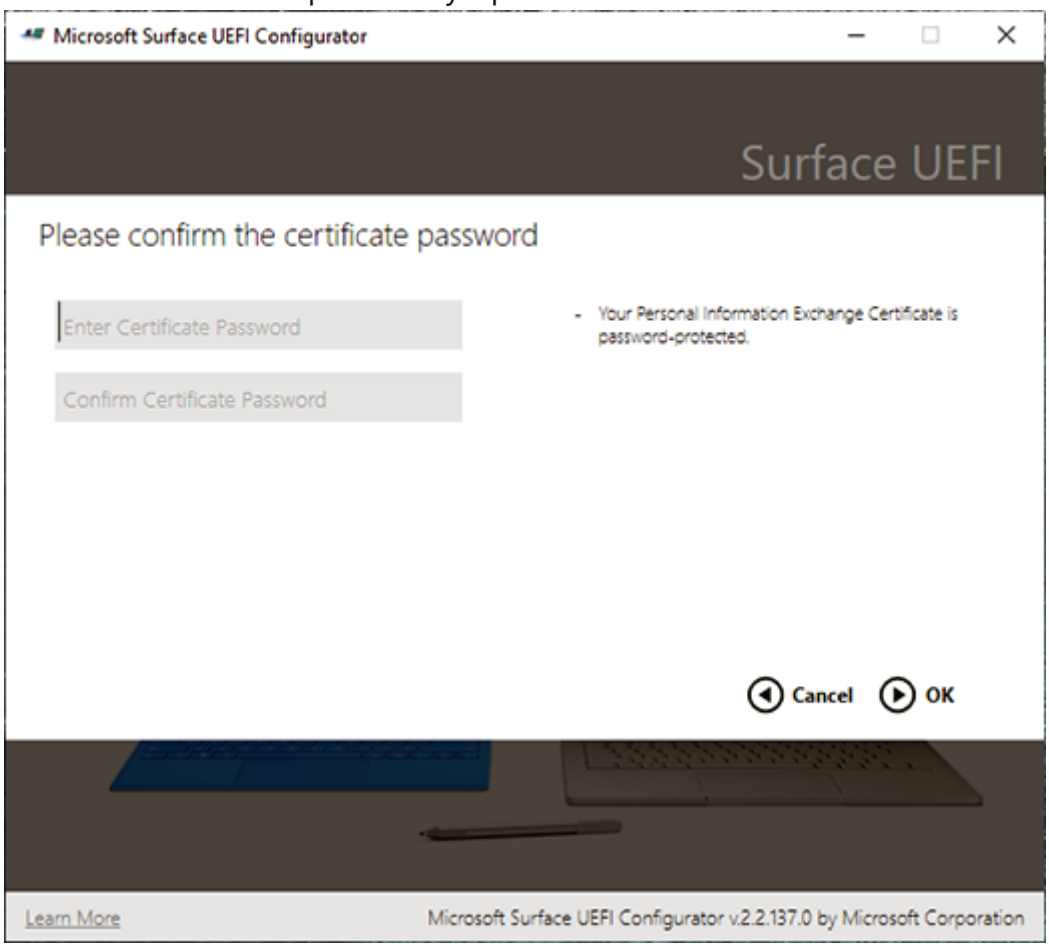


3. To add the certificate to your package, you must have a valid certificate with the private key in a .pfx file format to sign and protect the package. Select +

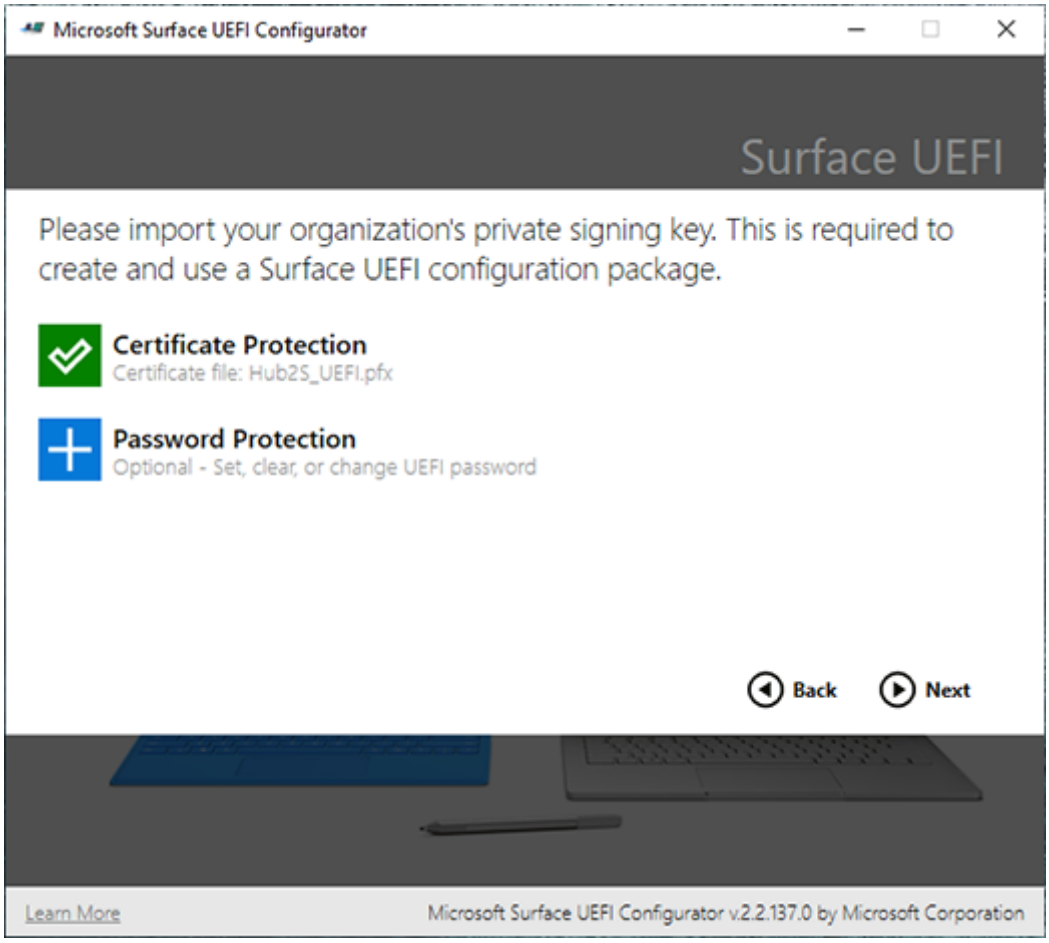
Certificate Protection.



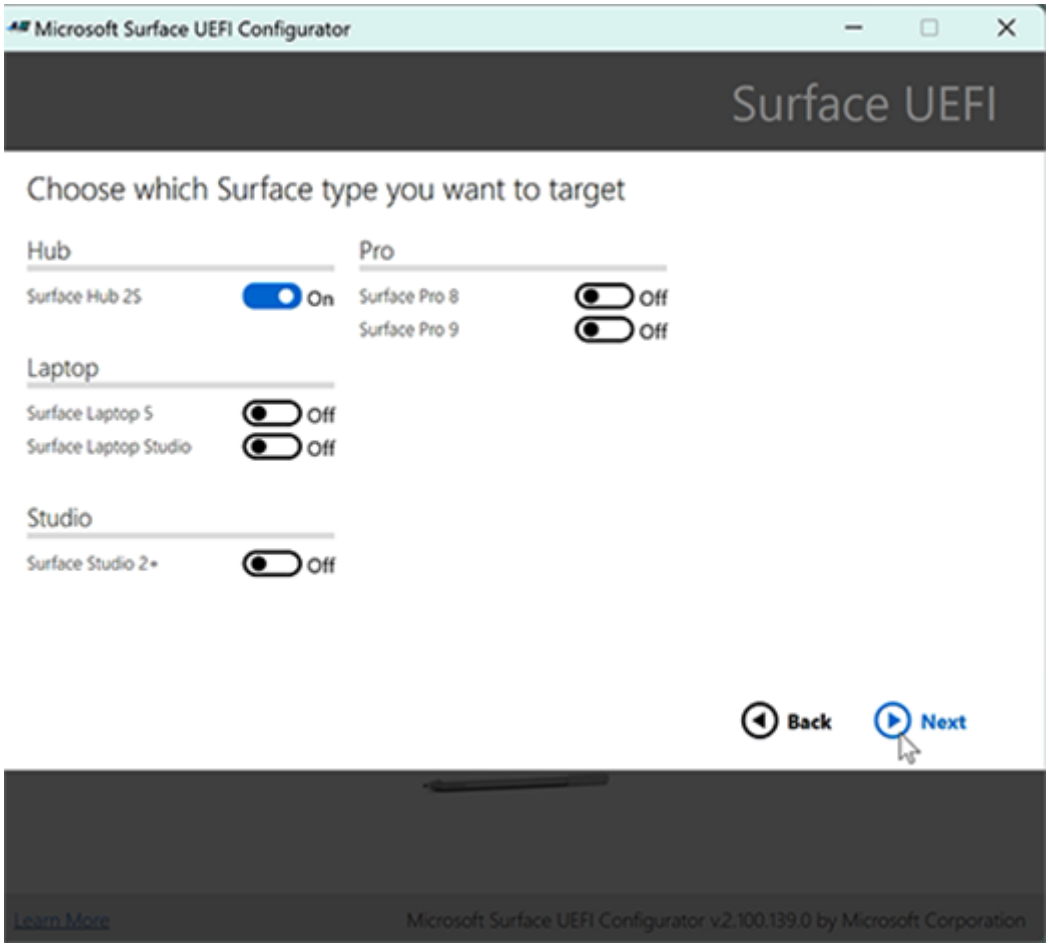
4. Enter the certificate's private key's password.



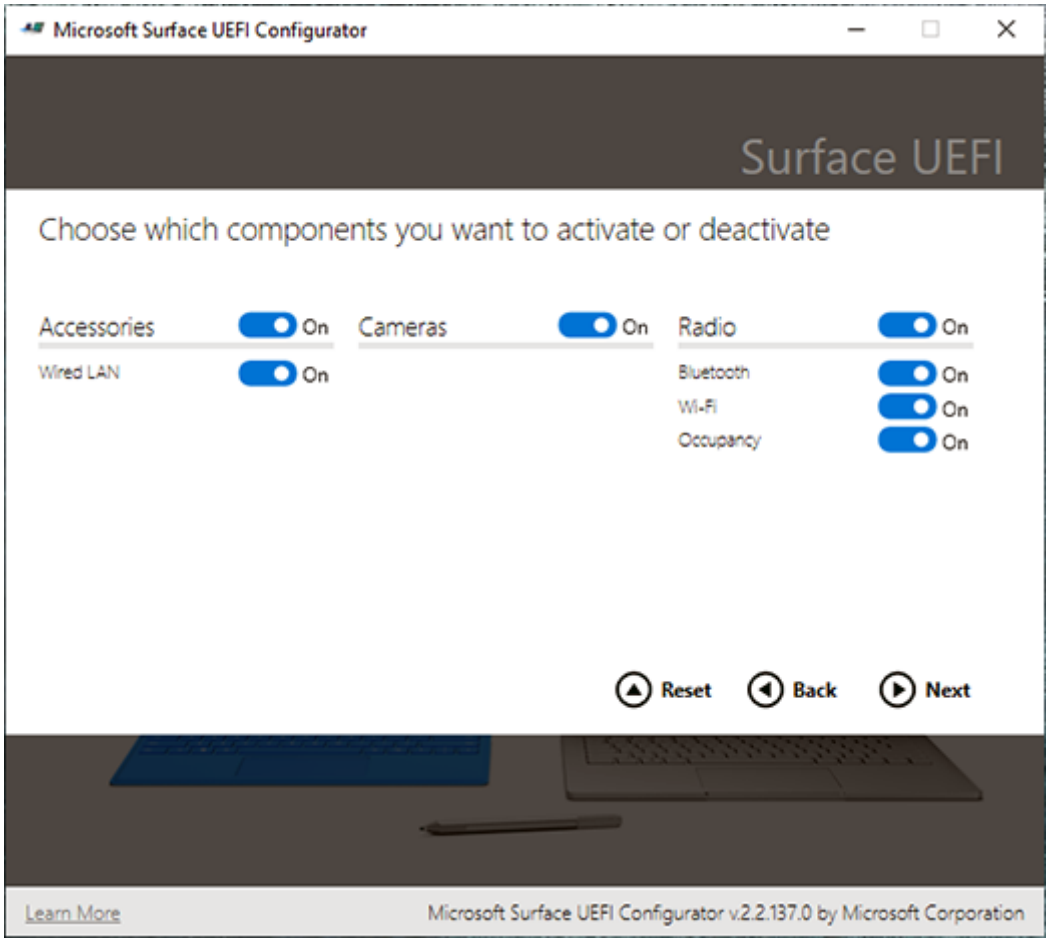
5. After importing the private key, continue creating the package.



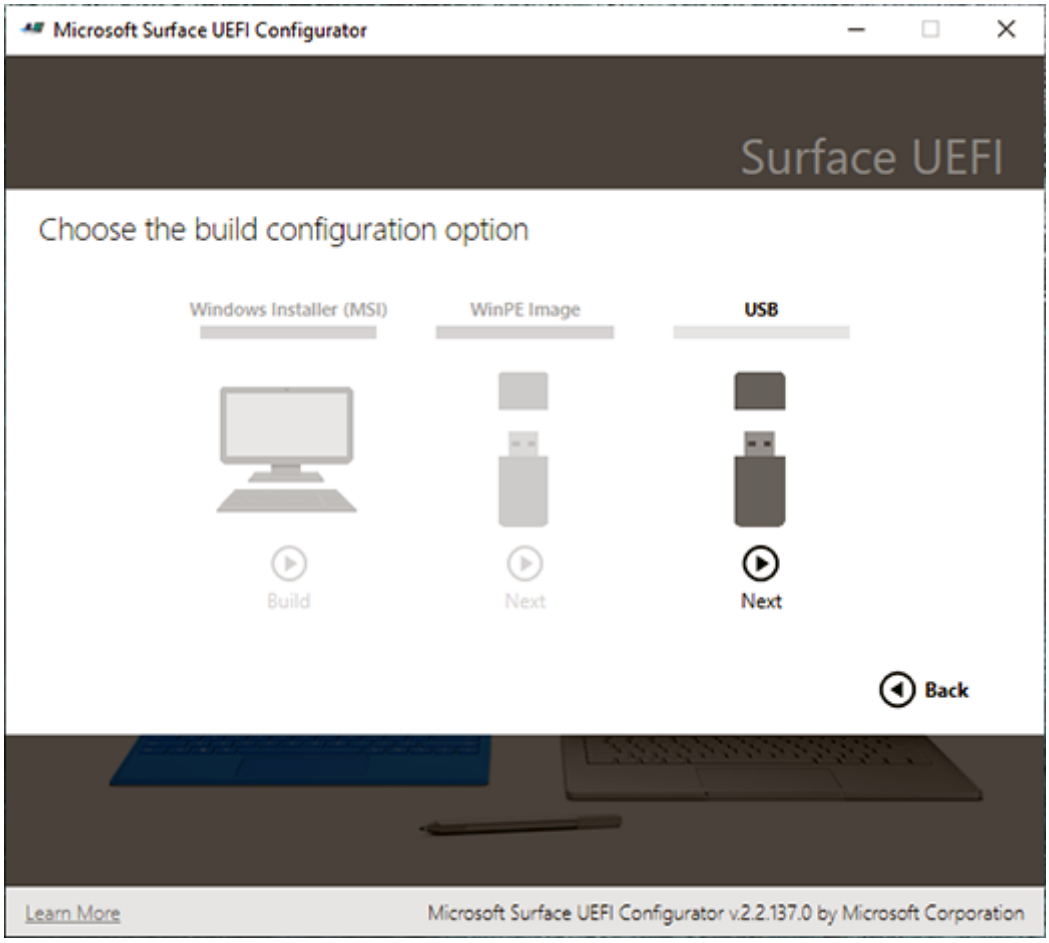
6. Choose **Surface Hub 2S** as the target for the UEFI configuration package.



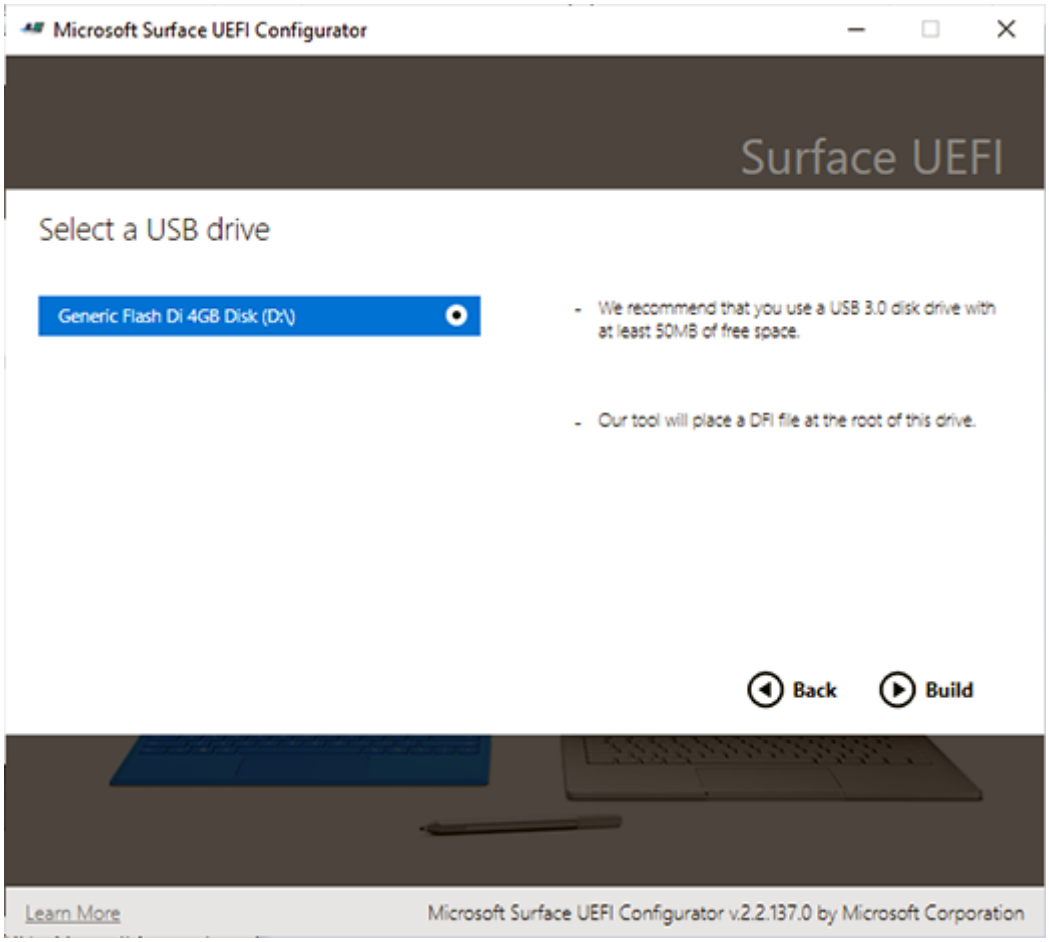
7. Choose the components and settings you want to activate or deactivate on Surface Hub 2S.



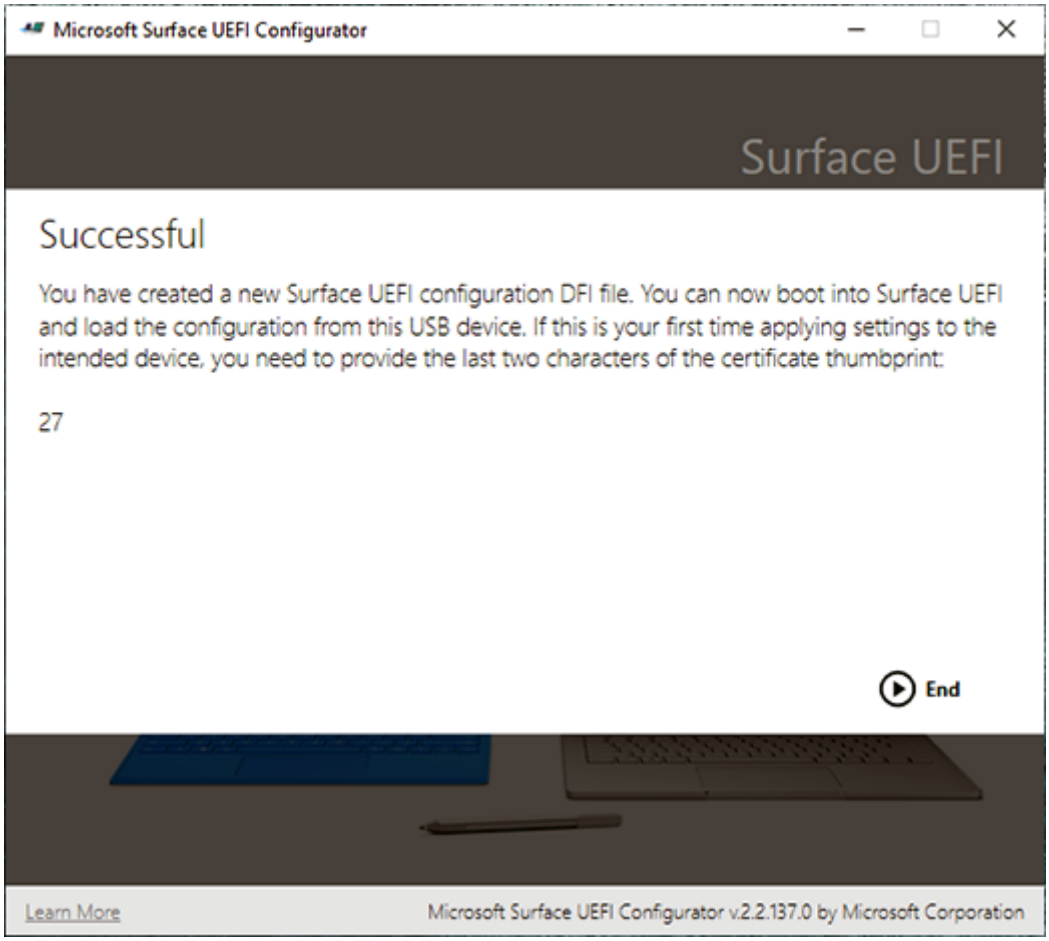
8. Use the USB option to export the file.



9. Insert and choose the USB drive you'd like to use for this package. The USB drive will be formatted and you lose any information you have on it.



10. Upon successful creation of the package, the Configurator will display the last two characters of your certificate's thumbprint. You need these characters when you import to the configuration to Surface Hub 2S.



To boot into UEFI

Turn off Surface Hub 2S. Press and hold the **Volume Up** button and press the **Power** Button. Keep holding the Volume Up button until the UEFI menu appears.

Surface Hub update history

Article • 03/21/2023

Windows was designed to be a service, which means it automatically gets better through periodic software updates. Typically you don't have to do anything to get the latest Windows 10 updates—they'll download and install whenever they're available.

Most Windows updates focus on performance and security improvements. In the list below, the most recent Windows update with Surface Hub-specific improvements is listed first. Updates are cumulative, so installing the latest available Windows update (even if it isn't on the list below) ensures that you also benefit from improvements in any previous updates. Microsoft Store apps are updated through the Microsoft Store (managed by the Surface Hub's system administrator). Details about app updates are provided on a per-app basis.

> **Tip**
>
> This page is refreshed as new updates are released. Please refer to the **Surface Hub Important Information** page for related topics on current and past releases that may require your attention.

Windows 10 Team 2022 Update (22H2)

April 25, 2023 - update for Team OS based on KB5025297* (19045.2913)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves an issue where the Surface Hub password rotation feature did not work as expected with Azure AD-based device accounts.
- Updates the built-in Azure Log Analytics agent to version 10.20.18067.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5025297

March 21, 2023 - update for Team OS based on KB5023773* (19045.2788)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves an issue where Meetings and Files sign-in could take a long time in some proxy environments.
- Resolves an issue where End Session cleanup could unnecessarily trigger a restart of the device.
- Implements a feature that allows end users to change the preferred display language on the device.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5023773

January 19, 2023 - update for Team OS based on KB5019275* (19045.2546)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves an issue where meeting invitations did not show up immediately on the Welcome screen calendar in some environments without a reboot.
- Resolves an issue where one-click meeting join from the Welcome screen calendar did not automatically join Teams meetings in GCC High environments.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5019275

November 15, 2022 - update for Team OS based on KB5020030* (19045.2311)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Replaces built-in email client on Surface Hub with a new one to enable more share via email scenarios.
- Improves sovereign cloud support by adding tenant region awareness to some personal sign-in and device account scenarios.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5020030

October 25, 2022 - update for Team OS based on KB5018482* (19045.2193)

This update brings the Windows 10 Team 2022 Update to Surface Hub and includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves an issue where Surface Hub devices did not advertise Miracast availability in some scenarios.

Please refer to the "Install Windows 10 Team 2022 Update" page for more information regarding update availability by region, distribution method, and device type.
*KB5018482

Windows 10 Team 2020 Update (20H2)

August 26, 2022 - update for Team OS based on KB5016688* (19042.1949)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves an issue where Teams or Skype for Business Quality of Service settings did not apply DSCP markings as expected.
- Update to allow the Edge (Chromium) browser to launch the File Explorer app when clicking on the Downloads folder icon.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5016688

August 24, 2022 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Surface UEFI update - 697.178.768.0
  - Improves system security and stability.
- Surface ME Firmware update - 11.8.92.4222
  - Improves system security and stability.
- Intel(R) Management Engine Interface driver - 2145.1.42.0
  - Improves system security and stability.

June 2, 2022 - update for Team OS based on KB5014023* (19042.1741)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves an issue where the Welcome screen calendar did not show a "Join" action for Teams meetings in GCC High environments.
- Resolves an issue where a "Microsoft Teams is not responding" window would sometimes appear during regular Teams usage.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5014023

May 19, 2022 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Intel(R) graphics driver - 30.0.101.1339
  - Improves system stability.
- Intel(R) Ethernet driver - 12.19.1.37
  - Improves system stability.
- Surface SMC Firmware update - 4.3.139.0
  - Improves Surface Hub 2 Smart Camera performance in different lighting conditions.
- Surface UEFI update - 697.148.768.0
  - Improves thermal logging and detection of thermal shutdown scenarios.

April 21, 2022 - update for Team OS based on KB5011831* (19042.1682)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Fix that prevents "End Session" from triggering the message "Your device needs an update. Restarting to finish it up..." and subsequent restart in some scenarios.
- Fix that ensures the SurfaceHub CSP can be used with SyncML policies that configure Device Accounts in `DOMAIN\username` format.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5011831

March 22, 2022 - update for Team OS based on KB5011543* (19042.1620)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Adds ability for administrators to install Progressive Web Apps (PWAs).
- Resolves an issue where some Surface Hubs joined to Azure AD or configured with a local administrator account could fail to synchronize their computer clock.
- Resolves an issue where using Meetings and Files sign-in suggestions with the Authenticator app could force the user to repeat the login process.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5011543

February 15, 2022 - update for Team OS based on KB5010415* (19042.1566)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub are outlined in Windows 10 Team 2020 Update 2, and also include the below:

- Fix that allows Exchange services to be disabled during Device Account setup.
- Improves reliability for some Device Account setup scenarios when using an on-premises Exchange mailbox.
- Improves reliability for some MDM policy setting scenarios when using the SurfaceHub CSP.
- Improves reliability for incoming call scenarios when using Skype for Business.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5010415

January 25, 2022 - update for Team OS based on KB5009596* (19042.1503)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves an issue where Surface Hubs could not report data to their configured Azure Log Analytics workspaces.
- Resolves an issue where starting a Skype for Business meeting from a Surface Hub's Welcome screen could result in a fully maximized SfB client that was not

minimizable.
- Resolves an issue where Azure AD-joined Surface Hubs did not pre-populate Meetings and Files sign-in with a list of meeting invitees.
- Resolves an issue where device account password rotation could not be enabled in some on-premises scenarios.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5009596

January 21, 2022 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Surface UEFI update - 694.3924.768.0
  - Improves system security and stability.
- Intel(R) Management Engine Interface driver - 2120.100.0.1085
  - Improves system security and stability.

November 22, 2021 - update for Team OS based on KB5007253* (19042.1387)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Fix that enforces a 32-character limit when using MDM policy to set 'Friendly Name' on a Surface Hub.
- Fix that corrects AllowStorageCard MDM policy behavior when it is reverted back to a value of 1 (storage cards allowed) from 0.
- Update to allow the Edge (Chromium) browser to access the same file locations accessible in File Explorer, including an attached USB drive.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5007253

September 30, 2021 - KB5004196, KB5004198, and KB5004199

These updates to the Surface Hub deliver the Teams Room client, Teams Admin Center agent, and Managed Meeting Rooms agent. Key features are outlined in Teams Room on Surface Hub.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services.

September 30, 2021 - update for Team OS based on KB5005611* (19042.1266)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Replaces Meeting Mode 1 (Teams preferred/SfB available) with Mode 2 functionality (Teams only); either setting can be used, but both have the same effect.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5005611

September 1, 2021 - update for Team OS based on KB5005101* (19042.1202)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub are outlined in Windows 10 Team 2020 Update 1 and also include the below:

- Improves reliability for some Device Account setup scenarios when using an on-premises Exchange mailbox.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5005101

July 29, 2021 - update for Team OS based on KB5004296* (19042.1151)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Update to the "Collect logs" feature to include Windows diagnostic data in csv format.
- Fix that ensures that End Session cleanup fully removes all data related to Edge Chromium.
- Improves some personal sign-in scenarios with Azure AD-joined Surface Hubs when using the Authenticator app.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5004296

June 10, 2021 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Surface UEFI update - 694.3751.768.0
  - Addresses critical security vulnerability and improves system stability.
- Surface ME Firmware update - 11.8.86.3877
  - Addresses critical security vulnerability and improves system stability.
- Intel(R) Management Engine Interface driver - 2102.100.0.1044
  - Addresses critical security vulnerability and improves system stability.

April 13, 2021 - update for Team OS based on KB5001330* (19042.928)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves an issue where some Surface Hub devices were only installing monthly Windows security updates, instead of all Windows cumulative updates.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB5001330

March 13, 2021 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Intel(R) Bluetooth driver - 22.30.0.4
  - Improves system security and stability.
- Intel(R) graphics driver - 27.20.100.8682
  - Improves system security and stability.
- Intel(R) Wi-Fi driver - 22.30.0.11
  - Improves system security and stability.

February 2, 2021 - update for Team OS based on KB4598291* (19042.789)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Fix that allows calendar synchronization with Exchange to work when the Device Account's UPN is not equal to its SMTP address.
- Adds ability for administrators to disable the use of Modern Authentication during calendar synchronization with Exchange.
- Ensures that Surface Hub users aren't prompted to enter proxy credentials after the "Use device account credentials" feature has been enabled.
- Resolves an issue where Windows Update and Store update checks would never complete if a proxy requiring authentication was in use.
- Improves the reliability of the Connect App during wired ingest scenarios.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4598291

January 15, 2021 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Surface SMC Firmware update - 3.93.139.0
- Surface UEFI update - 694.3473.768.0

December 11, 2020 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Surface SMC Firmware update - 3.92.139.0
- Surface UEFI update - 694.3447.768.0

November 30, 2020 - update for Team OS based on KB4586853* (19042.662)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Update to Privacy Settings page to provide additional options.
- Resolves an issue where meetings that had already started were not displayed on Welcome/Start screen.
- Resolves an issue with cloud recovery for non-en-US locales.

- Skype for Business
  - Improves directional audio performance.
  - Reduced “pen tap” sounds when using Pen during Skype for Business calls.
- Improves reliability when enrolling into Windows Insider Program.
- Improves reliability of Windows Team shell.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4586853

November 24, 2020 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Surface SMC Firmware update - 3.91.139.0
  - Improve connected standby reliability.
- Surface Touch Firmware update - 3.91.139.0
  - Improve connected standby touch response.
- Surface USB Audio Firmware update - 3.91.139.0
- Surface Pen Firmware update - 3.91.139.0

October 27, 2020 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Surface System Aggregator Firmware update - 4.14.139.0
- Surface UEFI update - 694.3386.768.0

October 13, 2020 - update for Team OS based on KB4579311* (19042.572)

Windows 10 Team 2020 Update for Surface Hub - General Release notes

This update brings the Windows 10 Team 2020 Update to Surface Hub and includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, are noted on the page "What's new in Windows 10 Team 2020 Update".

*KB4579311

Windows 10 Team Creators Update (1703)

September 1, 2020 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Surface SMC Firmware update - 1.177.139.0
  - Improves field repair scenarios.
- Surface SSD Firmware update - 5.14.139.0
  - Improves system stability.
- Surface Serial Hub driver - 9.40.139.0
  - Improves system stability.

May 4, 2020 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Surface USB audio driver - 15.3.6.0
  - Improves directional audio performance.
- Intel(R) display audio driver - 10.27.0.5
  - Improves screen sharing scenarios.
- Intel(R) graphics driver - 26.20.100.7263
  - Improves system stability.
- Surface System driver - 1.7.139.0
  - Improves system stability.
- Surface SMC Firmware update - 1.176.139.0
  - Improves system stability.

February 28, 2020 - update for Surface Hub 2S

This update is specific to the Surface Hub 2S and provides the driver and firmware updates outlined below:

- Surface Integration driver - 13.46.139.0
  - Improves display brightness scenarios.
- Intel(R) Management Engine Interface driver - 1914.12.0.1256
  - Improves system stability.
- Surface SMC Firmware update - 1.161.139.0
  - Improves pen battery performance.

- Surface UEFI update - 694.2938.768.0
  - Improves system stability.

February 11, 2020 - update for Team OS based on KB4537765* (15063.2284)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves an issue where the Hub 2S can't be heard well by other participants during Skype for Business calls.
- Improves reliability for some Arabic, Hebrew, and other RTL language usage scenarios on Surface Hub.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4537765

January 14, 2020 - update for Team OS based on KB4534296* (15063.2254)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Addresses an issue with log collection for Microsoft Surface Hub 2S.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4534296

September 24, 2019 - update for Team OS based on KB4516059* (15063.2078)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Update to Surface Hub 2S Recovery Settings page to accurately reflect recovery options.
- Update to Surface Hub 2S Welcome screen to improve device recognizability.
- Addressed an issue with the Windows Team shell background displaying incorrectly.
- Addressed an issue with Start Menu layout persistence when configured using MDM policy.

- Fixed an issue in Microsoft Edge that occurs when browsing some internal websites.
- Fixed an issue in Skype for Business that occurs when presenting in full-screen mode.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4516059

August 17, 2019 - update for Team OS based on KB4512474* (15063.2021)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Ensures that Video Out on Hub 2S defaults to "Duplicate" mode.
- Improves reliability for some Arabic language usage scenarios on Surface Hub.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4512474

June 18, 2019 - update for Team OS based on KB4503289* (15063.1897)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Addresses an issue preventing a user from signing in to a Microsoft Surface Hub device with an Azure Active Directory account. This issue occurs because a previous session did not end successfully.
- Adds support for TLS 1.2 connections to identity providers and Exchange in device account setup scenarios.
- Fixes to improve reliability of Hardware Diagnostic App on Hub 2S.
- Fix to improve consistency of first-run setup experience on Hub 2S.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4503289

May 28, 2019 - update for Team OS based on KB4499162* (15063.1835)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Ensures that Surface Hub users aren't prompted to enter proxy credentials after the "Use device account credentials" feature has been enabled.
- Resolves an issue where Skype connections fail periodically because audio/video isn't using the correct proxy.
- Adds support for TLS 1.2 in Skype for Business.
- Resolves a SIP connection failure in the Skype client when the Skype server has TLS 1.0 or TLS 1.1 disabled.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4499162

April 25, 2019 - update for Team OS based on KB4493436* (15063.1784)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves video and audio sync issue with some USB devices that are connected to the Surface Hub.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4493436

November 27, 2018 - update for Team OS based on KB4467699* (15063.1478)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Addresses an issue that prevents some users from Signing-In to “My Meetings and Files.”

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4467699

October 18, 2018 - update for Team OS based on KB4462939* (15063.1418)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Skype for Business fixes:
  - Resolves Skype for Business connection issue when resuming from sleep
  - Resolves Skype for Business network connection issue, when device is connected to Internet
  - Resolves Skype for Business crash when searching for users from directory
- Resolves issue where the Hub mistakenly reports “No Internet connection” in enterprise proxy environments.
- Implemented a feature allowing customers to opt in to a new Whiteboard experience.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4462939

August 31, 2018 - update for Team OS based on KB4343889* (15063.1292)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Adds support for Microsoft Teams
- Resolves task management issue with Intune registration
- Enables Administrators to disable Instant Messaging and Email services for the Hub
- Additional bug fixes and reliability improvements for the Surface Hub Skype for Business App

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4343889

June 21, 2018 - update for Team OS based on KB4284830* (15063.1182)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Telemetry change in support of GDPR requirements in EMEA

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4284830

April 17, 2018 - update for Team OS based on KB4093117* (15063.1058)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves a wired projection issue
- Enables bulk update for certain MDM (Mobile Device Management) policies
- Resolves phone dialer issue with international calls
- Addresses image resolution issue when two Surface Hubs join the same meeting
- Resolves OMS (Operations Management Suite) certificate handling error
- Addresses a security issue when cleaning up at the end of a session
- Addresses Miracast issue, when Surface Hub is specified to channels 149 through 165
    - Channels 149 through 165 will continue to be unusable in Europe, Japan or Israel due to regional governmental regulations

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4093117

February 23, 2018 - update for Team OS based on KB4077528* (15063.907)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolved an issue where MDM settings were not being correctly applied
- Improved Cleanup process

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4077528

January 16, 2018 - update for Team OS based on KB4057144* (15063.877)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Adds ability to manage Start Menu tile layout via MDM
- MDM bug fix on password rotation configuration

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4057144

December 12, 2017 - update for Team OS based on KB4053580* (15063.786)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves camera video flashes (tearing or flickers) during Skype for Business calls
- Resolves Notification Center SSD ID issue

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4053580

November 14, 2017 - update for Team OS based on KB4048954* (15063.726)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Feature update that allows customers to enable 802.1x wired network authentication using MDM policy.
- A feature update that enables users to dynamically select an application of their choice when opening a file.
- Fix that ensures that End Session cleanup fully removes all connections between the user's account and the device.
- Performance fix that improves cleanup time as well as Miracast connection time.
- Introduces Easy Authentication utilization during ad-hoc meetings.
- Fix that ensures proxy settings configured on the device are used across all service components.
- Reduces and more thoroughly secures the telemetry transmitted by the device, reducing bandwidth utilization.
- Enables a feature allowing users to provide feedback to Microsoft after a meeting concludes.

Please refer to the Surface Hub Admin guide for enabling/disabling device features and services. *KB4048954

October 10, 2017 - update for Team OS based on KB4041676* (15063.674)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Skype for Business
  - Resolves issue that required a device reboot when resuming from sleep.
  - Fixes issue where external contacts did not resolve through Skype Online Hub account.
- PowerPoint
  - Fixes problem where some PowerPoint presentations would not project on Hub.
- General
  - Fix to resolve issue where USB port could not be disabled by System Administrator.

*KB4041676

September 12, 2017 - update for Team OS based on KB4038788* (15063.605)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Security
  - Resolves issue with BitLocker when device wakes from sleep.
- General
  - Reduces frequency/amount of device health telemetry, improving system performance.
  - Fixes issue that prevented device from collecting system logs.

*KB4038788

August 1, 2017 - update for Team OS based on KB4032188* (15063.498)

- Skype for Business
  - Resolves Skype for Business Sign-In issue, which required retry or system reboot.
  - Resolves Skype for Business meeting time being incorrectly displayed.
  - Fixes to improve Surface Hub Skype for Business reliability.

*KB4032188

June 27, 2017 - update for Team OS based on KB4022716* (15063.442)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Address NVIDIA driver crashes that may necessitate sleeping 84" Surface Hub to power down, requiring a manual restart.
- Resolved an issue where some apps fail to launch on an 84" Surface Hub.

*KB4022716

June 13, 2017 - update for Team OS based on KB4022725* (15063.413)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- General
  - Resolved Pen ink dropping issues with pens
  - Resolved issue causing extended time to "cleanup" meeting

*KB4022725

May 24, 2017 - update for Team OS based on KB4021573* (15063.328)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- General
  - Resolved issue with proxy setting retention during update issue

*KB4021573

May 9, 2017 - update for Team OS based on KB4016871* (15063.296)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- General

    - Addressed sleep/wake cycle issue
    - Resolved several Reset and Recovery issues
    - Addressed Update History tab issue
    - Resolved Miracast service launch issue
- Apps
    - Fixed App package update error

*KB4016871

Windows 10 Team Creators Update 1703 for Surface Hub - General Release notes (15063.0)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Evolving the large screen experience
    - Improved the meeting carousel in Welcome and Start
    - Join meetings and end the session directly from the Start menu
    - Apps can utilize more of the screen during a session
    - Simplified Skype controls
    - Improved mechanisms for providing feedback
- Access My Personal Content*
    - Personal single sign-on from Welcome or Start
    - Join meetings and end the session directly from the Start menu
    - Access personal files through OneDrive for Business directly from Start
    - Pre-populated attendee sign-in
    - Streamlined authentication flows with the "Authenticator" app
- Deployment & Manageability
    - Simplified OOBE experience through bulk provisioning
    - Cloud-based device recovery service
    - Enterprise client certificate support
    - Improved proxy credential support
    - Added and improved Skype Quality of Service (QoS) configuration support
    - Added ability to set default device volume in Settings
    - Improved MDM support for Surface Hub settings
- Improved Security
    - Added ability to restrict USB drives to BitLocker only
    - Added ability to disable USB drives via MDM
    - Added ability to disable "Resume session" functionality on timeout
    - Addition of wired 802.1x support
- Audio and Projection

    - Dolby Audio "Human Speaker" enhancements
    - Added support for Miracast infrastructure connections
- Reliability and Performance fixes
    - Resolved several Reset and Recovery issues
    - Resolved Surface Hub Exchange authentication issue when utilizing client certificates
    - Improved Wi-Fi network connection and credentials stability
    - Fixed Miracast audio popping and sync issues during video playback
    - Included setting to disable auto connect behavior

*Single sign-in feature requires use of Office 365 and OneDrive for Business

Windows 10 Team Anniversary Update (1607)

March 14, 2017 - update for Team OS based on KB4013429* (14393.953)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- General
    - Security fix for File Explorer to prevent navigation to restricted file locations
- Skype for Business
    - Fix to address latency during Remote Desktop based screen sharing

*KB4013429

January 10, 2017 - update for Team OS based on KB4000825* (14393.693)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Enabled selection of 106/109 Keyboard Layouts for use with physical Japanese keyboards

*KB4000825

December 13, 2016 - update for Team OS based on KB3206632* (14393.576)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Resolves wired connection audio distortion issue

*KB3206632

November 4, 2016 - update for Team OS based on KB3200970* (14393.447)

This update to the Windows 10 Team Anniversary Update (version 1607) for Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Skype for Business bug fixes to improve reliability

*KB3200970

October 25, 2016 - update for Team OS based on KB3197954* (14393.351)

This update to the Surface Hub includes quality improvements and security fixes. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Enabling new Sleep feature in OS and Bios to reduce the Surface Hub's power consumption and improve its long-term reliability
- General
  - Resolves scenarios where the on-screen keyboard would sometimes not appear
  - Resolves Whiteboard application shift that occasionally occurs when opening scheduled meeting
  - Resolves issue that prevented Admins from changing the local administrator password, after device has been reset
  - BIOS change to resolve an issue with status bar tracking during device reset
  - UEFI update to resolve powering down issues

*KB3197954

October 11, 2016 - update for Team OS based on KB3194496* (14393.222)

This update brings the Windows 10 Team Anniversary Update to Surface Hub and includes quality improvements and security fixes. (Your device will be running Windows

10 Version 1607 after it's installed.) Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Skype for Business
  - Performance improvements when joining meetings, including issues when joining a meeting using federated accounts
  - Video Based Screen Sharing (VBSS) support now available on Skype for Business for Surface Hub
  - Resolved disconnection after 5 minutes of idle time issue
  - Resolved Skype Hub-to-Hub screen sharing failure
  - Improvements to Skype video, including:
    - Loss of video during meeting with multiple video presenters
    - Video cropping during calls
    - Outgoing call video not displaying for other participants
  - Addressed issue with UPN sign-in error
  - Addressed issue with dial pad during use of Session Initiation Protocol (SIP) calls
- Whiteboard
  - User can now save and recall Whiteboard sessions using OneDrive online service (via Share functionality)
  - Improved launching Whiteboard when removing pen from dock
- Apps
  - Pre-installed OneDrive app, for access to your personal and work files
  - Pre-installed Photos app, to view photos and video
  - Pre-installed Power BI app, to view dashboards
  - The Office apps – Word, Excel, PowerPoint – are all ink-enabled
  - Edge on Surface Hub now supports Flash-based websites
- General
  - Enabled Audio Device Selection (for Surface Hubs attached using external audio devices)
  - Enabled support for HDCP on DisplayPort output connector
  - System UI changes to settings for usability optimization (refer to User and Admin Guides for additional details)
  - Bug fixes and performance optimizations to speed up the Azure Active Directory sign-in flow
  - Reduced time needed to reset and restore a Surface Hub
  - Windows Defender UI has been added within settings
  - Improved UX touch to start
  - Enabled support for greater than 1080p wireless projection via Miracast, on supported devices
  - Resolved "There's no internet connection" and "Appointments may be out of date" false notification states from launch

    - Improved reliability of on-screen keyboard
    - Additional support for creating Surface Hub provisioning packages using Windows Imaging & Configuration Designer (ICD) and improved Surface Hub monitoring solution on Operations Management Suite (OMS)

*KB3194496

Updates for Windows 10 Version 1511

July 12, 2016 - update for Team OS based on KB3172985* (10586.494)

This update includes quality improvements and security fixes. No new operating system features are being introduced in this update. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Fixed issue that caused Windows system crashes
- Fixed issue that caused repeated Edge crashes
- Fixed issue causing pre-shutdown service crashes
- Fixed issue where some app data wasn't properly removed after a session
- Updated Broadcom NFC driver to improve NFC performance
- Updated Marvell Wi-Fi driver to improve Miracast performance
- Updated Nvidia driver to fix a display bug in which 84" Surface Hub devices show dim or fuzzy content
- Numerous Skype for Business issues fixed, including:
    - Issue that caused Skype for Business to disconnect during meetings
    - Issue in which users were unable to join meetings when the meeting organizer was on a federated configuration
    - Enabling Skype for Business application sharing
    - Issue that caused Skype application crashes
- Added a prompt in "Settings" to inform users that the OS can become corrupted if device reset is interrupted before completion

*KB3172985

May 10, 2016 - update for Team OS based on KB3156421* (10586.318)

This update to the Surface Hub includes quality improvements and security fixes. No new operating system features are being introduced in this update. Key updates to

Surface Hub, not already outlined in Windows 10 Update History, include:

- Fixed issue that prevented certain Store apps (OneDrive) from installing
- Fixed issue that caused touch input to stop responding in applications

*KB3156421

April 12, 2016 - update for Team OS based on KB3147458* (10586.218)

This update to the Surface Hub includes quality improvements and security fixes. No new operating system features are being introduced in this update. Key updates to Surface Hub, not already outlined in Windows 10 Update History, include:

- Fixed issue where volume level wasn't properly reset between sessions

*KB3147458

Related topics

- Windows 10 release information
- Windows 10 November update: FAQ
- Microsoft Surface update history
- Microsoft Lumia update history
- Get Windows 10

Known issues: Windows 10 Team

Article • 06/13/2023

This article lists known issues for Surface Hubs running the current operating system, Windows 10 Team Edition version 22H2.

To ensure Surface Hub receives the latest updates, sign in with an Admin account and select **All apps** > **Settings** > **Update and Security** > **Windows Update**, and then install all updates.

Issue	Description	Remedy
Adding a device account with an Exchange Online mailbox may fail during the first-run experience.	Exchange Online began disabling basic authentication for all protocols as of October 1st, 2022. Windows 10 Team edition does fully support modern authentication, but only as of KB5010415 (or a subsequent Windows CU).	One of the following options can be used to address this scenario: - Download the latest Hub 2S recovery image and follow the USB recovery steps to update your Surface Hub and go through the first-run experience again. - Skip setting up a device account in the first-run process, install all Windows Updates afterwards, and then add the account from **Settings** > **Surface Hub** > **Accounts**.
Authentication of hybrid device accounts with on-premises mailboxes fails.	Surface Hub devices default to using Modern Authentication for accounts that exist in Azure AD, even if they have mailboxes in on-premises Exchange environments that don't have Hybrid Modern Authentication enabled. In this scenario, the account authentication fails. As a result, it may not be possible to add a new device account or sync an existing one.	After KB4598291 (or a subsequent Windows CU) is installed, the SurfaceHub CSP has a new ExchangeModernAuthEnabled parameter available to toggle the use of Modern Authentication. This can be set to false via MDM policy or provisioning package to prevent the Hub from using Modern Authentication.

Issue	Description	Remedy
Some Surface Hubs may stop synchronizing their computer clock with time.windows.com if they have been affiliated with Azure Active Directory or configured with no affiliation. When this synchronization is not working, time on the device may drift from the actual time.	Clock drift beyond 5 minutes can cause authentication failures in standard Surface Hub scenarios including Teams sign-in.	On the impacted device, go to **All Apps** > **Settings** > **Time & language** > **Date & time**, and toggle **Set time automatically** off, then back on. Microsoft is actively looking to find a resolution to this issue.
Some Surface Hubs may fail to fully resume from power-saving states such as sleep.	When waking up, one of the intermediate states the Hub goes through displays a black screen with the Windows logo. In this scenario, the device stays on that screen.	As a workaround, the Hub can be turned off and back on by holding the physical power button. Microsoft is actively looking to find a resolution to this issue.
Some Surface Hub 2S devices may experience a tonal / hissing sound during Teams calls.	In some situations, the built-in mic array can pick up unwanted environmental sounds.	One of the following workarounds can be used: - Set Noise Suppression to High in Teams. - Connect an audio peripheral to the Hub to use as the default microphone. A future update to the Hub's Teams client will improve the default noise cancellation behavior.
Surface Hub 2S devices are unable to receive driver updates using WSUS.	Surface Hub 2S supports Windows Update and Windows Update for Business to distribute drivers; distribution via Windows Server Update Services (WSUS) is not supported.	If using WSUS, migrate to Windows Update for Business. **Learn more**: What is Windows update for business?

Issue	Description	Remedy
Some ease-of-access settings persist after a session ends	When users turn on the High contrast toggle either from the Quick actions menu or from the Settings app, this toggle persists after the user session ends. Similarly, if users change the notifications display to indicate 7 seconds versus the admin-defined 5 seconds, it remains 7 seconds, even though other settings are reset to the admin-defined values.	Users can turn off the High Contrast toggle from the quick actions(caret) menu accessible on the Taskbar soon after launching a session on the Hub. Display duration of notifications can be set to a different value via the Settings app by the next user - this setting is accessible to all users.

Troubleshoot Microsoft Surface Hub

Article • 01/03/2023

Troubleshoot common problems, including setup issues, Exchange ActiveSync errors.

The Surface Hub Hardware Diagnostic tool contains interactive tests which allow you to confirm essential functionality of your Hub is working as expected. In addition to testing hardware, the diagnostic can test the resource account to verify that it is configured properly for your environment. If problems are encountered, results can be saved and shared with the Surface Hub Support Team. For usage information, see Using the Surface Hub Hardware Diagnostic Tool to test a device account.

Common issues are listed in the following table, along with causes and possible fixes. The Setup troubleshooting section contains a listing of on-device problems, along with several types of issues that may be encountered during the first-run experience. The Exchange ActiveSync errors section lists common errors the device may encounter when trying to synchronize with an Microsoft Exchange ActiveSync server.

Setup troubleshooting

This section lists causes, and possible fixes to help troubleshoot issues you might find when you set up your Microsoft Surface Hub.

On-device

Possible fixes for issues on the Surface Hub after you've completed the first-run program.

Issue	Causes	Possible fixes
Not receiving automatic accept/decline messages.	The device account isn't configured to automatically accept/decline messages.	Use PowerShell cmdlet `Set-CalendarProcessing $upn -AutomateProcessing AutoAccept`.
	The device account isn't configured to process external meeting requests.	Use PowerShell cmdlet `Set-CalendarProcessing $upn -ProcessExternalMeetingMessages $true`.

Calendar is not showing on the Welcome screen, or message "Appointments of date (no account provisioned)" is being displayed.	No device account is set up on this Surface Hub.	Provision a device account through Settings.
Calendar is not showing on the Welcome screen or message "Appointments of date (overprovisioned)" is being displayed.	The device account is provisioned on too many devices.	Remove the device account from other devices that it's provisioned to. This can be done using the Exchange admin portal.
Calendar is not showing on the Welcome screen or message "Appointments of date (invalid credentials)" is being displayed.	The device account's password has expired and is no longer valid.	Update the account's password in Settings. Also see Password management.
Calendar is not showing on the Welcome screen or message "Appointments of date (account policy)" is being displayed.	The device account is using an invalid ActiveSync policy.	Make sure the device account has an ActiveSync policy where `PasswordEnabled == False`.
Calendar is not showing on the Welcome screen or message "Appointments may be out of date" is being displayed.	Exchange is not enabled.	Enable the device account for Exchange services through Settings. You need to make sure you have the right set of ActiveSync policies and have also installed any necessary certificates for Exchange services to work.
Can't log in to Skype for Business.	The device account does not have a Session Initiation Protocol (SIP) address property.	The account does not have a SIP address property and its User Principal Name (UPN) does not match the actual SIP address. The account must have its SIP address set, or the SIP address should be added using the Settings app.
Can't log in to Skype for Business.	The device account requires a certificate to authenticate into Skype for Business.	Install the appropriate certificate using provisioning packages.

First run

Possible fixes for issues with Surface Hub first-run program.

Issue	Causes	Possible fixes
Cannot find account when asked for domain and user name.	Domain needs to be the fully qualified domain name (FQDN).	The FQDN should be provided in the domain field.

Device account page, issues for new account settings

Issue	Causes	Possible fixes
Unable to find the provided account in Azure AD.	The provided account's User Principal Name (UPN) has a tenant that can't be reached in Azure AD.	Make sure that you have a working Internet connection, and that the device can reach Microsoft Online Services. Make sure the account credentials are entered correctly.
Unable to reach the specified directory.	The provided account domain specifies a domain that can't be reached.	Make sure that you have a working network connection, and that the device can reach the domain controller. Make sure the account credentials are entered correctly. You can also try using the FQDN instead.
Can't auto-discover Exchange server.	The Exchange server isn't configured for auto-discovery.	Enable auto-discovery of the Exchange server for the device account, or enter the account's Exchange server address manually.
Could not discover the SIP address after entering the account credentials.	There was no SIP address entry in Active Directory or Azure AD.	Make sure the account is enabled with Skype for Business and has a SIP address. If not, you can enter the SIP address manually into the text box.

Device account page, issues for existing account settings

Issue	Causes	Error codes	Possible fixes
Account could not	The account is not enabled as	None	Make sure the

authenticate with the specified credentials.	a user in Active Directory (AD), needs a password to authenticate, or the password is incorrect.		credentials are entered correctly. Enable the account as a user in AD and add a password, or set the RoomMailboxPassword.
Error 0x800C0019 is displayed when providing an Exchange server.	The device account requires a certificate to authenticate.	0x800C0019	Install the appropriate certificate using provisioning packages.
Device account credentials are not valid for the provided Exchange server.	The provided Exchange server is not where the device account's mailbox is hosted.	None	Make sure you are providing the correct Exchange mail server for the device account.
HTTP timeout while trying to reach Exchange server.		0x80072EE2	
Couldn't find the provided Exchange server.	The Exchange server provided could not be found.	None	Ensure that you have a working network or Internet connection, and that the Exchange server you provided is correct.
http not supported.	An Exchange server with *http://* instead of *https://* was provided.	None	Use an Exchange server that uses https.
People land on the page titled "There's a problem with this account" regarding ActiveSync.	The ActiveSync policy PasswordEnabled is set to True (or 1).	None	Create a new ActiveSync policy where PasswordEnabled is set to False (or 0), and then apply that policy to the account.
	The Surface Hub doesn't have a connection to Exchange.	None	Make sure that you have a working network or Internet connection.
	Exchange returns a status code indicating an error.	None	Make sure that you have a working network or Internet connection.

First run, Domain join page issues

Issue	Causes	Possible fixes
When trying to join a domain, an error shows that the account couldn't authenticate using the specified credentials.	The credentials provided are not capable of joining the specified domain.	Enter correct credentials for an account that exists in the specified domain.
When specifying a group from a domain, an error shows that the group couldn't be found on the domain.	The group may have been removed or no longer exists.	Verify that the group exists within the domain.

First run, Exchange server page

Issue	Causes	Possible fixes
People land on this page and are asked for the Exchange server address.	The Exchange server isn't configured for auto-discovery.	Enable auto-discovery of the Exchange server for the device account, or enter the account's Exchange server address manually.

First run, On-device issues

Issue	Causes	Error codes	Possible fixes
Can't sync mail/calendar.	The account has not allowed the Surface Hub as an allowed device.	0x86000C1C	Add the Surface Hub device ID to the allowed list by setting the **ActiveSyncAllowedDeviceIds** property for the mailbox.

Exchange ActiveSync errors

This section lists status codes, mapping, user messages, and actions an admin can take to solve Exchange ActiveSync errors.

Hex Code	Mapping	User-Friendly Message	Action admin should take

Hex Code	Mapping	User-Friendly Message	Action admin should take
0x85010002	E_HTTP_DENIED	The password must be updated.	Update the password.
0x80072EFD	WININET_E_CANNOT_CONNECT	Can't connect to the server right now. Wait a while and try again, or check the account settings.	Verify that the server name is correct and reachable. Verify that the device is connected to the network.
0x86000C29	E_NEXUS_STATUS_DEVICE_NOTPROVISIONED (policies don't match)	The account is configured with policies not compatible with Surface Hub.	Disable the **PasswordEnabled** policy for this account. We have a bug were we may surface policy errors if the account doesn't receive any server notifications within the policy refresh interval.
0x86000C4C	E_NEXUS_STATUS_MAXIMUMDEVICESREACHED	The account has too many device partnerships.	Delete one or more partnerships on the server.
0x86000C0A	E_NEXUS_STATUS_SERVERERROR_RETRYLATER	Can't connect to the server right now.	Wait until the server comes back online. If the issue persists, re-provision the account.

Hex Code	Mapping	User-Friendly Message	Action admin should take
0x85050003	E_CREDENTIALS_EXPIRED (Credentials have expired and need to be updated)	The password must be updated.	Update the password.
0x8505000D	E_AIRSYNC_RESET_RETRY	Can't connect to the server right now. Wait a while or check the account's settings.	This is normally a transient error but if the issue persists check the number of devices associated with the account and delete some of them if the number is large.
0x86000C16	E_NEXUS_STATUS_USER_HASNOMAILBOX	The mailbox was migrated to a different server.	You should never see this error. If the issue persists, re-provision the account.
0x85010004	E_HTTP_FORBIDDEN	Can't connect to the server right now. Wait a while and try again, or check the account's settings.	Verify the server name to make sure it is correct. If the account is using cert based authentication make sure the certificate is still valid and update it if not.
0x85030028	E_ACTIVESYNC_PASSWORD_OR_GETCERT	The account's password or client certificate are missing or invalid.	Update the password and/or deploy the client certificate.

Hex Code	Mapping	User-Friendly Message	Action admin should take
0x86000C2A	E_NEXUS_STATUS_DEVICE_POLICYREFRESH	The account is configured with policies not compatible with Surface Hub.	Disable the PasswordEnabled policy for this account.
0x85050002	E_CREDENTIALS_UNAVAILABLE	The password must be updated.	Update the password.
0x80072EE2	WININET_E_TIMEOUT	The network doesn't support the minimum idle timeout required to receive server notification, or the server is offline.	Verify that the server is running. Verify the NAT settings.
0x85002004	E_FAIL_ABORT	This error is used to interrupt the hanging sync, and will not be exposed to users. It will be shown in the diagnostic data if you force an interactive sync, delete the account, or update its settings.	Nothing.

Hex Code	Mapping	User-Friendly Message	Action admin should take
0x85010017	E_HTTP_SERVICE_UNAVAIL	Can't connect to the server right now. Wait a while or check the account's settings.	Verify the server name to make sure it is correct. Wait until the server comes back online. If the issue persists, re-provision the account.
0x86000C0D	E_NEXUS_STATUS_MAILBOX_SERVEROFFLINE	Can't connect to the server right now. Wait a while or check the account's settings.	Verify the server name to make sure it is correct. Wait until the server comes back online. If the issue persists, re-provision the account.
0x85030027	E_ACTIVESYNC_GETCERT	The Exchange server requires a certificate.	Import the appropriate EAS certificate on the Surface Hub.
0x86000C2B	E_NEXUS_STATUS_INVALID_POLICYKEY	The account is configured with policies not compatible with Surface Hub.	Disable the PasswordEnabled policy for this account. We have a bug were we may surface policy errors if the account doesn't receive any server notifications within the policy refresh interval.

Hex Code	Mapping	User-Friendly Message	Action admin should take
0x85010005	E_HTTP_NOT_FOUND	The server name is invalid.	Verify the server name to make sure it is correct. If the issue persists, re-provision the account.
0x85010014	E_HTTP_SERVER_ERROR	Can't connect to the server.	Verify the server name to make sure it is correct. Trigger a sync and, if the issue persists, re-provision the account.
0x80072EE7	WININET_E_NAME_NOT_RESOLVED	The server name or address could not be resolved.	Make sure the server name is entered correctly.
0x8007052F	ERROR_ACCOUNT_RESTRICTION	While auto-discovering the Exchange server, a policy is applied that prevents the logged-in user from logging in to the server.	This is a timing issue. Re-verify the account's credentials. Try to re-provision when they're correct.
0x800C0019	INET_E_INVALID_CERTIFICATE	Security certificate required to access this resource is invalid.	Install the correct ActiveSync certificate needed for the provided device account.

Hex Code	Mapping	User-Friendly Message	Action admin should take
0x80072F0D	WININET_E_INVALID_CA	The certificate authority is invalid or is incorrect. Could not auto-discover the Exchange server because a certificate is missing.	Install the correct ActiveSync certificate needed for the provided device account.
0x80004005	E_FAIL	The domain provided couldn't be found. The Exchange server could not be auto-discovered and was not provided in the settings.	Make sure that the domain entered is the FQDN, and that there is an Exchange server entered in the Exchange server text box.

Contact Support

If you have questions or need help, you can create a support request.

Related content

- Troubleshooting Miracast connection to the Surface Hub

Troubleshoot Azure AD Join on Surface Hub

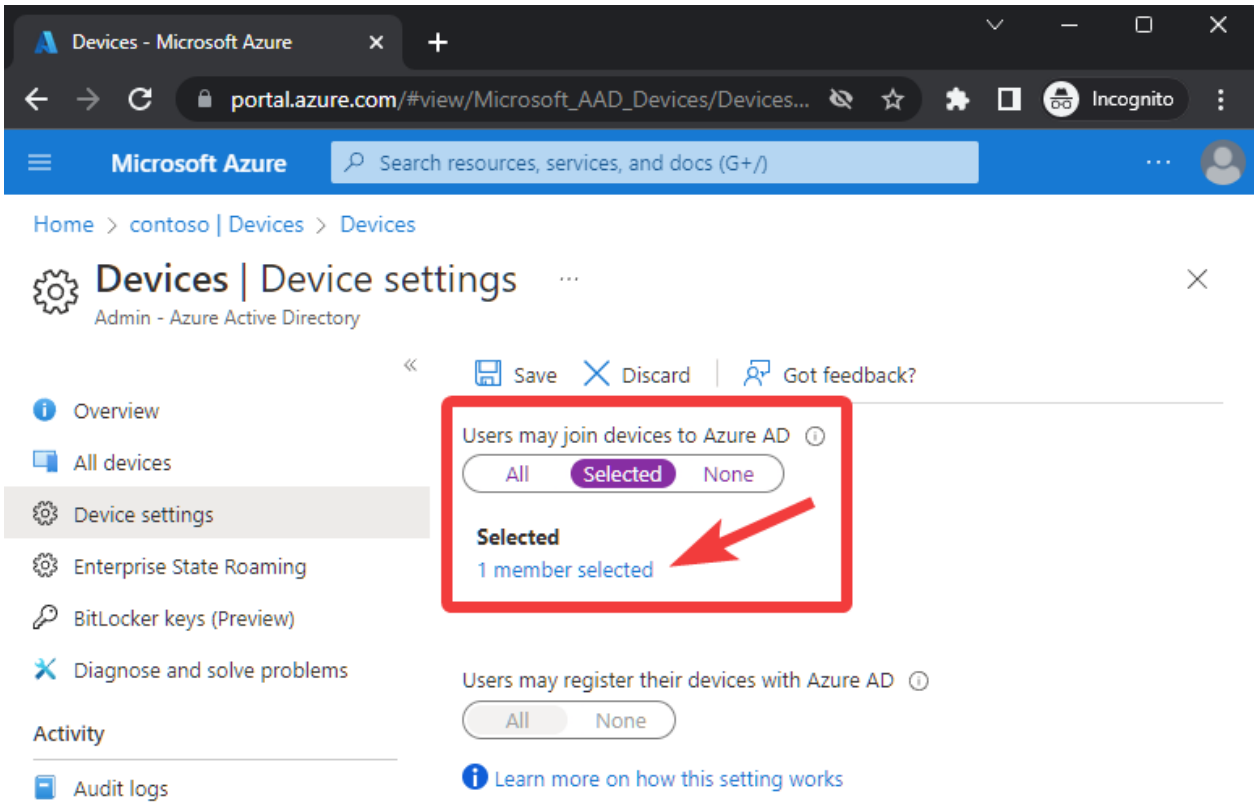
Article • 03/01/2023

If you can't join Surface Hub to Azure AD during the first run Out of Box Experience (OOBE), follow the troubleshooting guidance on this page.

Azure AD permissions

A common reason a user cannot join a device to Azure AD is related to Azure AD permissions. To confirm which users can join devices to Azure AD:

- Go to the Azure AD portal and select **Devices** > **Device settings**. Ensure "Users may join devices to Azure AD" is set to **All** or **Selected**. For Selected users, confirm the account used to join Azure AD is included in the assigned group.

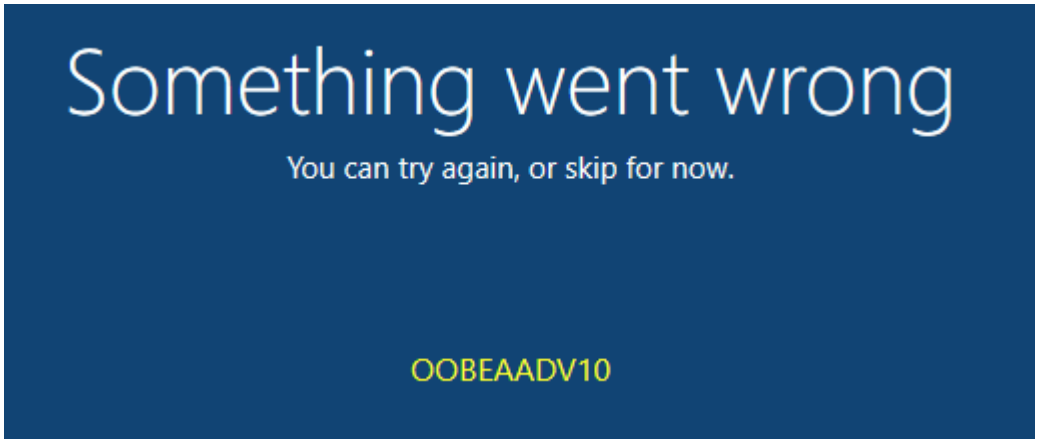


Maximum number of devices

Errors can also occur if the user exceeds the maximum number of devices allowed to join to Azure AD. If a user reaches this limit, they can't add more devices until one or more existing devices are removed. The default value is 50 devices and can be increased to 100 within Azure AD.

Unable to reach Azure AD

If error OOBEAADV10 is shown, the Surface Hub cannot reach the necessary Microsoft 365 endpoints. If encountered, follow the below troubleshooting steps in order.



Step	Troubleshooting Step	Purpose	Additional Information
1	If your organization uses a proxy, ensure the proxy settings and required certificates are installed on the Surface Hub.	Allows Surface Hub to reach necessary Microsoft endpoints to Azure AD join the device.	To configure proxy settings on a Surface Hub during OOBE, a provisioning package needs to be created and installed. If a certificate is required, refer to the instructions included in Create provisioning packages for Surface Hub.
2	Connect Surface Hub to a less restrictive network, such as a different VLAN, guest network or mobile Wi-Fi hotspot.	Using a less restrictive network may resolve the connectivity issue.	
3	Mirror network port the Surface Hub is using to capture and log network traffic. Analyze logs to determine if something is being blocked.	Third-party network packet capture software can't be installed natively on the Surface Hub. Mirroring the network port allows for this data to be captured.	Visit Office 365 URLs and IP address ranges for a detailed list of Microsoft endpoints that should be reachable.

Troubleshoot Azure Sign-in Logs for Surface Hub

Article • 04/24/2023

What are Azure sign-in logs?

Azure sign-in logs provide information on successful and failed sign-in attempts that occur within an Azure AD tenant. The Azure sign-in logs provide a detailed view of all sign-in activities for an account. When sign-in issues are encountered on the Surface Hub, an IT administrator can review these logs for any interrupts or failures. Here are some common reasons these logs are helpful to troubleshoot Surface Hub issues:

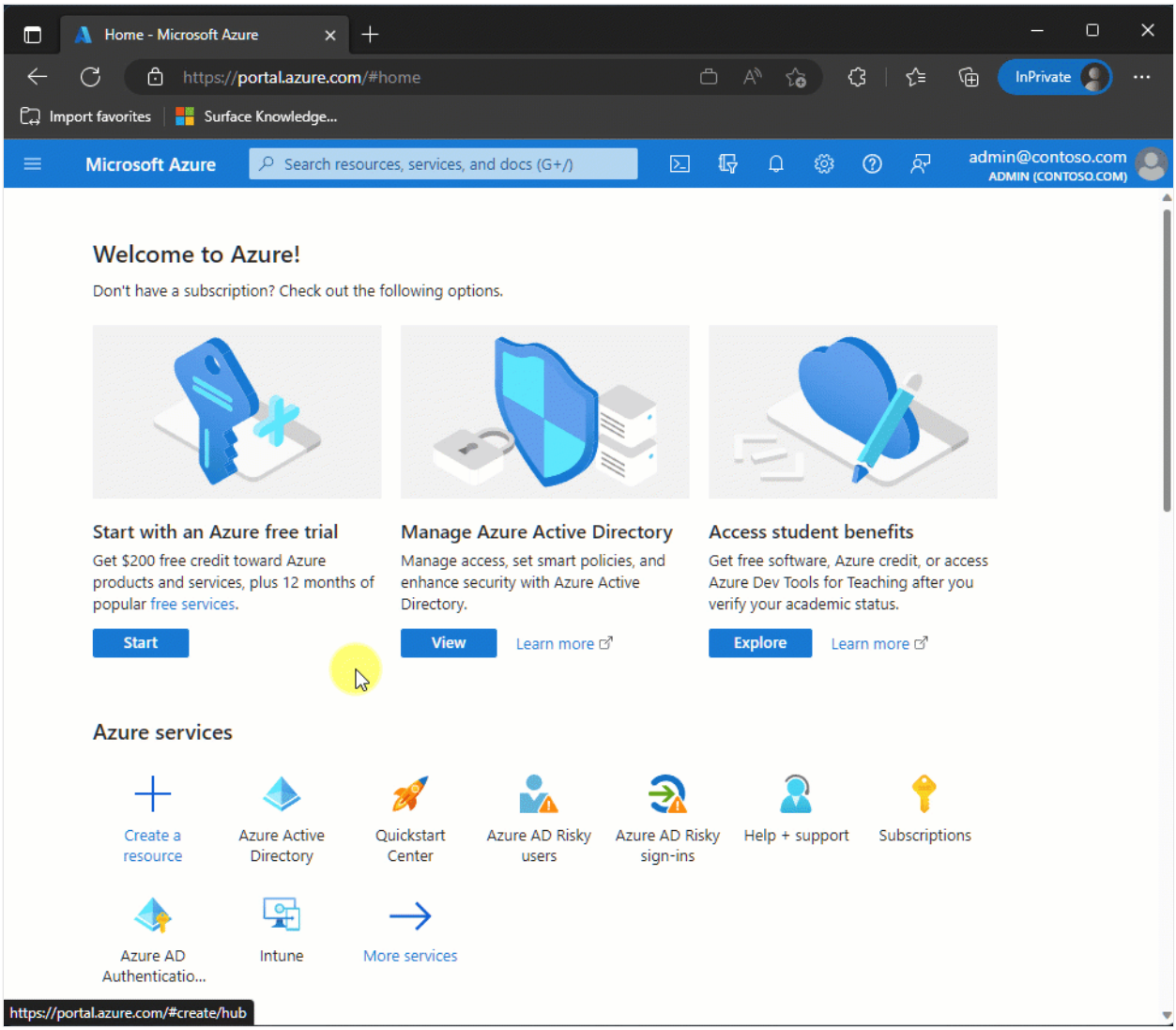
- Unable to add the device account to the Surface Hub
- Device account no longer syncs with Exchange Online
- Teams Rooms client fails to sign in
- Users unable to personally sign into the device

If you experience sign-in issues with the Surface Hub device account or personal user sign-in, follow the troubleshooting steps on this page.

View sign-in logs

To access the Azure sign-in logs for a tenant, a user must have the necessary role assigned.

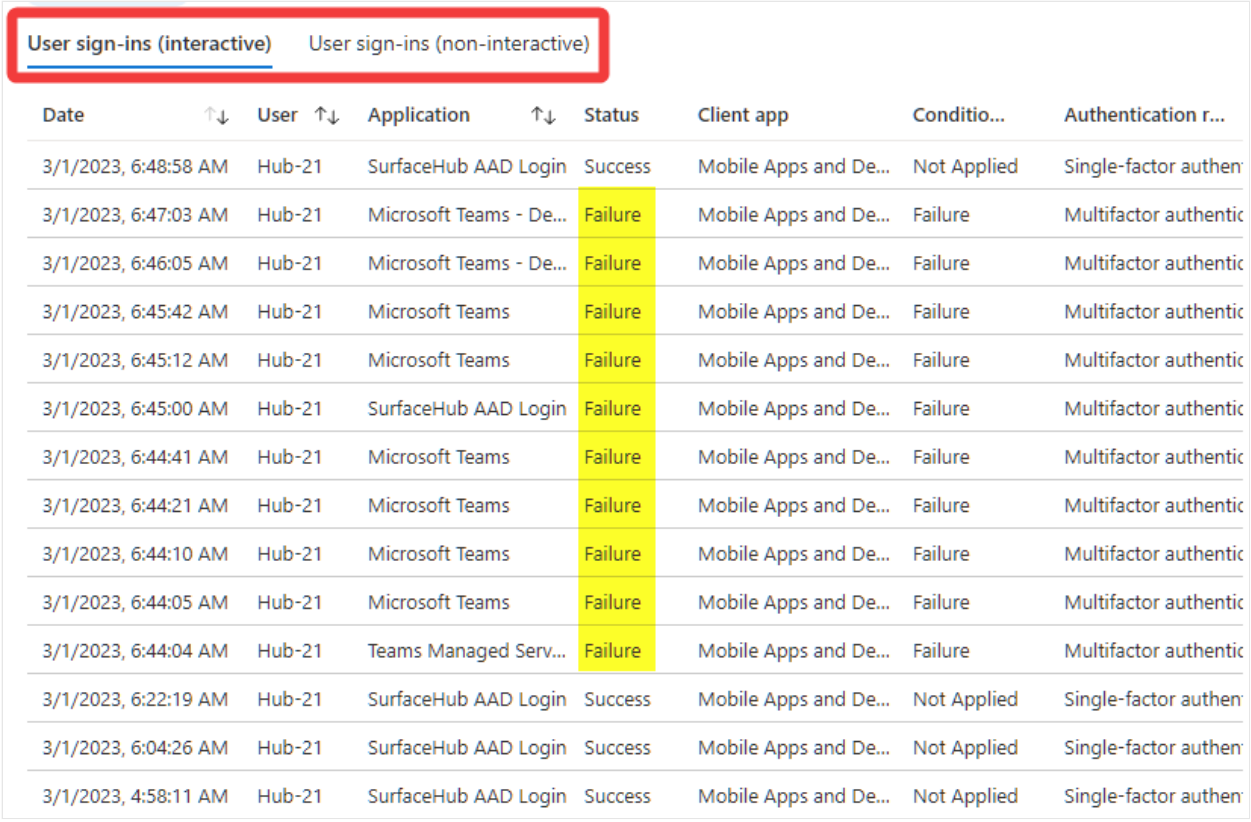
1. Sign in to the Azure portal
2. Go to **Azure Active Directory** > **Users**
3. Locate or search for the account you're troubleshooting and select it.
4. Select **Sign-in logs**
5. If you see a banner to **Try out our new sign-in preview**, select it.



> **Note**
>
> The sign-in logs may take 5-10 minutes to propagate to Azure.

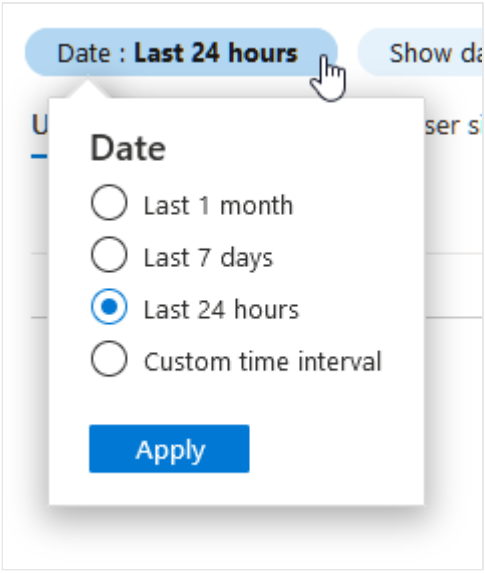
Analyze sign-in logs

Scroll through the interactive and non-interactive sign-in logs and note the **Status** column. If any failures or interrupts are seen, select the sign-in for additional details. You can optionally filter the sign-in logs by status to only show failures and interrupts.



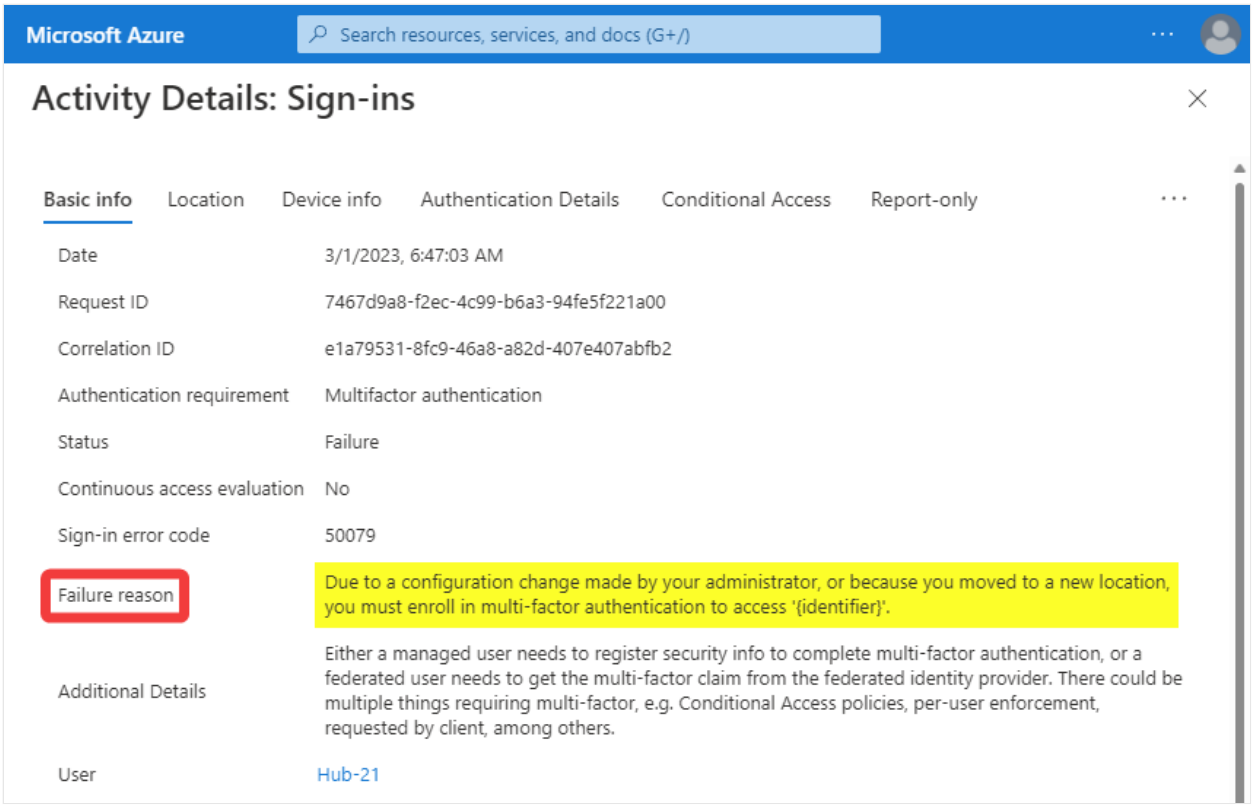
Date	User	Application	Status	Client app	Conditio...	Authentication r...
3/1/2023, 6:48:58 AM	Hub-21	SurfaceHub AAD Login	Success	Mobile Apps and De...	Not Applied	Single-factor authen
3/1/2023, 6:47:03 AM	Hub-21	Microsoft Teams - De...	Failure	Mobile Apps and De...	Failure	Multifactor authentic
3/1/2023, 6:46:05 AM	Hub-21	Microsoft Teams - De...	Failure	Mobile Apps and De...	Failure	Multifactor authentic
3/1/2023, 6:45:42 AM	Hub-21	Microsoft Teams	Failure	Mobile Apps and De...	Failure	Multifactor authentic
3/1/2023, 6:45:12 AM	Hub-21	Microsoft Teams	Failure	Mobile Apps and De...	Failure	Multifactor authentic
3/1/2023, 6:45:00 AM	Hub-21	SurfaceHub AAD Login	Failure	Mobile Apps and De...	Failure	Multifactor authentic
3/1/2023, 6:44:41 AM	Hub-21	Microsoft Teams	Failure	Mobile Apps and De...	Failure	Multifactor authentic
3/1/2023, 6:44:21 AM	Hub-21	Microsoft Teams	Failure	Mobile Apps and De...	Failure	Multifactor authentic
3/1/2023, 6:44:10 AM	Hub-21	Microsoft Teams	Failure	Mobile Apps and De...	Failure	Multifactor authentic
3/1/2023, 6:44:05 AM	Hub-21	Microsoft Teams	Failure	Mobile Apps and De...	Failure	Multifactor authentic
3/1/2023, 6:44:04 AM	Hub-21	Teams Managed Serv...	Failure	Mobile Apps and De...	Failure	Multifactor authentic
3/1/2023, 6:22:19 AM	Hub-21	SurfaceHub AAD Login	Success	Mobile Apps and De...	Not Applied	Single-factor authen
3/1/2023, 6:04:26 AM	Hub-21	SurfaceHub AAD Login	Success	Mobile Apps and De...	Not Applied	Single-factor authen
3/1/2023, 4:58:11 AM	Hub-21	SurfaceHub AAD Login	Success	Mobile Apps and De...	Not Applied	Single-factor authen

To analyze sign-in activity older than 24 hours, select the Date field to expand the timeframe.

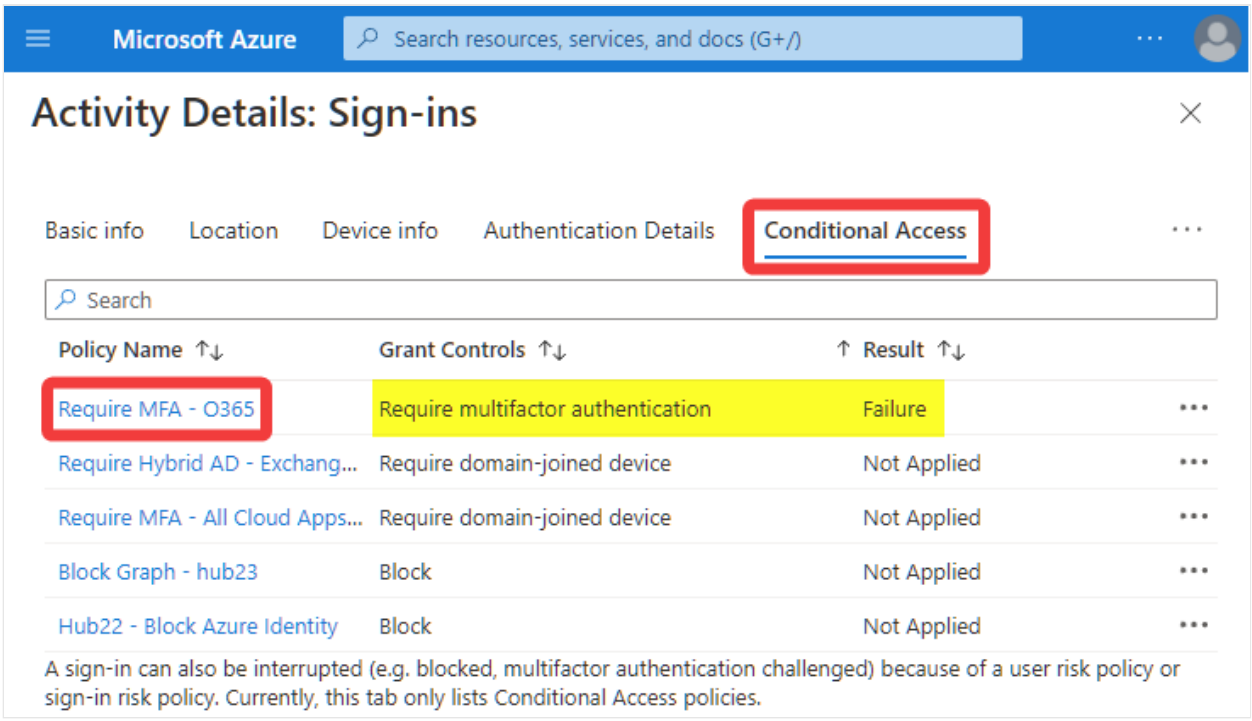


Additional sign-in details

After you select the sign-in, the activity details pane shows the reason for the failure or interrupt. In this example, the failure is caused by multi-factor authentication (MFA), which the Surface Hub device account doesn't support.



To reveal the policy that is enforcing MFA on the device account, select the Conditional Access tab.



Follow the guidance on Conditional Access for Surface Hub to better understand the requirements for the device, and how to exclude the device account from unsupported policies.

Additional details on how to view and analyze the Azure sign-in logs can be found on the Sign-in logs in Azure Active Directory page.

Conditional Access for Surface Hub

Article • 04/24/2023

What is Conditional Access?

Conditional Access is an Azure Active Directory (Azure AD) feature that allows organizations to configure policies to grant or block access to corporate resources. These policies are if-then statements, of Assignments and Access controls. If incompatible Conditional Access policies are enforced on the Surface Hub device account, you may experience one or more of the following issues:

- Unable to add the device account to the Surface Hub
- Welcome Screen calendar fails to sync with Exchange
- Teams Rooms client not signing in

Follow the guidance on this page to better understand how the Surface Hub device account interacts with Conditional Access and how to troubleshoot issues.

Device account and Conditional Access policies

The Surface Hub device account is used to receive meeting invitations and join Teams meetings. When creating Conditional Access policies, consider the below Surface Hub distinctions for Assignments and Access controls to prevent the device account from being blocked.

Assignments

Cloud apps

The Surface Hub device account uses the following cloud apps when signing in. Ensure your Conditional Access policies are configured to allow sign-in to these resources.

- Office 365
- Office 365 Exchange Online
- Office 365 SharePoint Online (this includes OneDrive for Business)
- Graph Explorer
- Microsoft Teams

Conditions

The Surface Hub is included in the following conditions.

- Device platforms - Windows
- Client apps - Mobile apps and desktop

Access controls

The Surface Hub device account isn't compatible with Conditional Access policies requiring the below types of Grant and Session Access controls. The device accounts for all Surface Hubs must be excluded from such policies.

Grant

- Require multifactor authentication
- Require authentication strength (Preview)
- Require device to be marked as compliant
- Require Hybrid Azure AD joined device
- Require approved client app
- Require app protection policy
- Require password change

Session

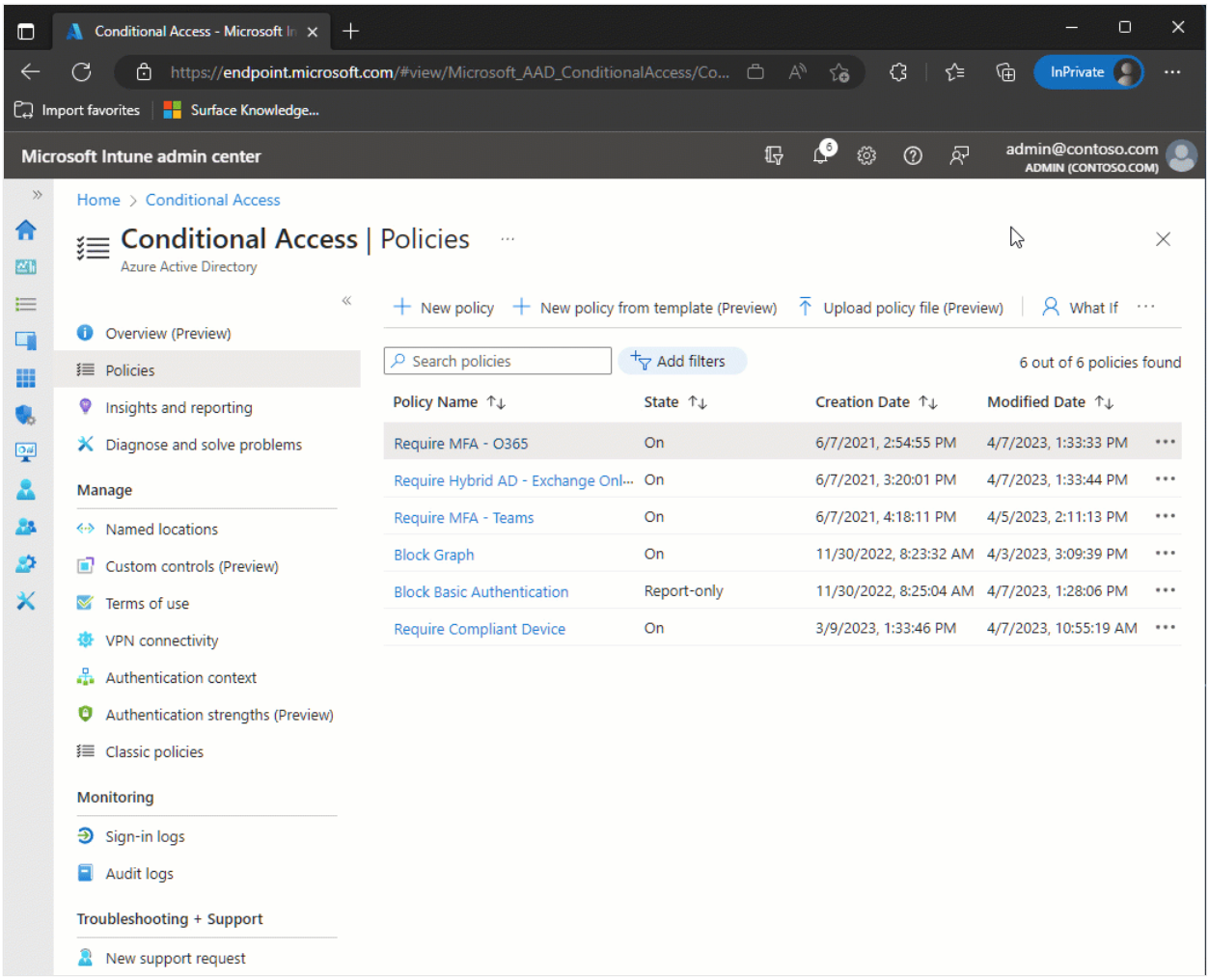
- Use app-enforced restrictions
- Use Conditional Access App Control

Additional details on Assignments and Access controls can be found in the building a Conditional Access policy article.

Troubleshoot

If your Surface Hub is experiencing sign-in issues with the device account, first review the Azure sign-in logs to determine if any failures or interrupts are seen. The details of the failed sign-in will typically show if a Conditional Access policy is blocking sign-in.

The "What If" tool can be used to determine which Conditional Access policies apply to the device account. When using the tool, select the Surface Hub device account as the user and leave the default "Any cloud app." More information can be found at Troubleshooting Conditional Access using the What If tool.



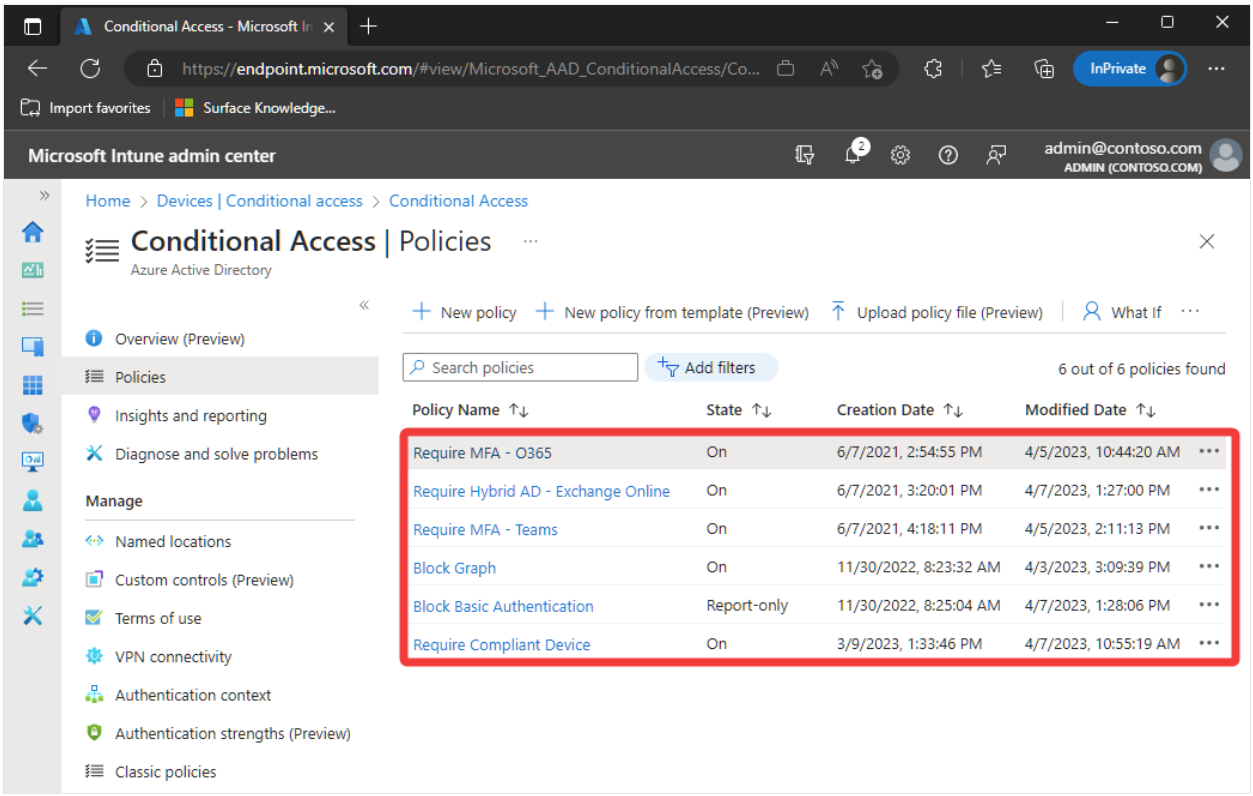
Review Conditional Access Policies

If the Azure sign-in logs and "What If" tool don't reveal any Conditional Access policies affecting the account, it's recommended to manually review every Conditional Access policy to ensure the Surface Hub device account isn't affected.

Step 1

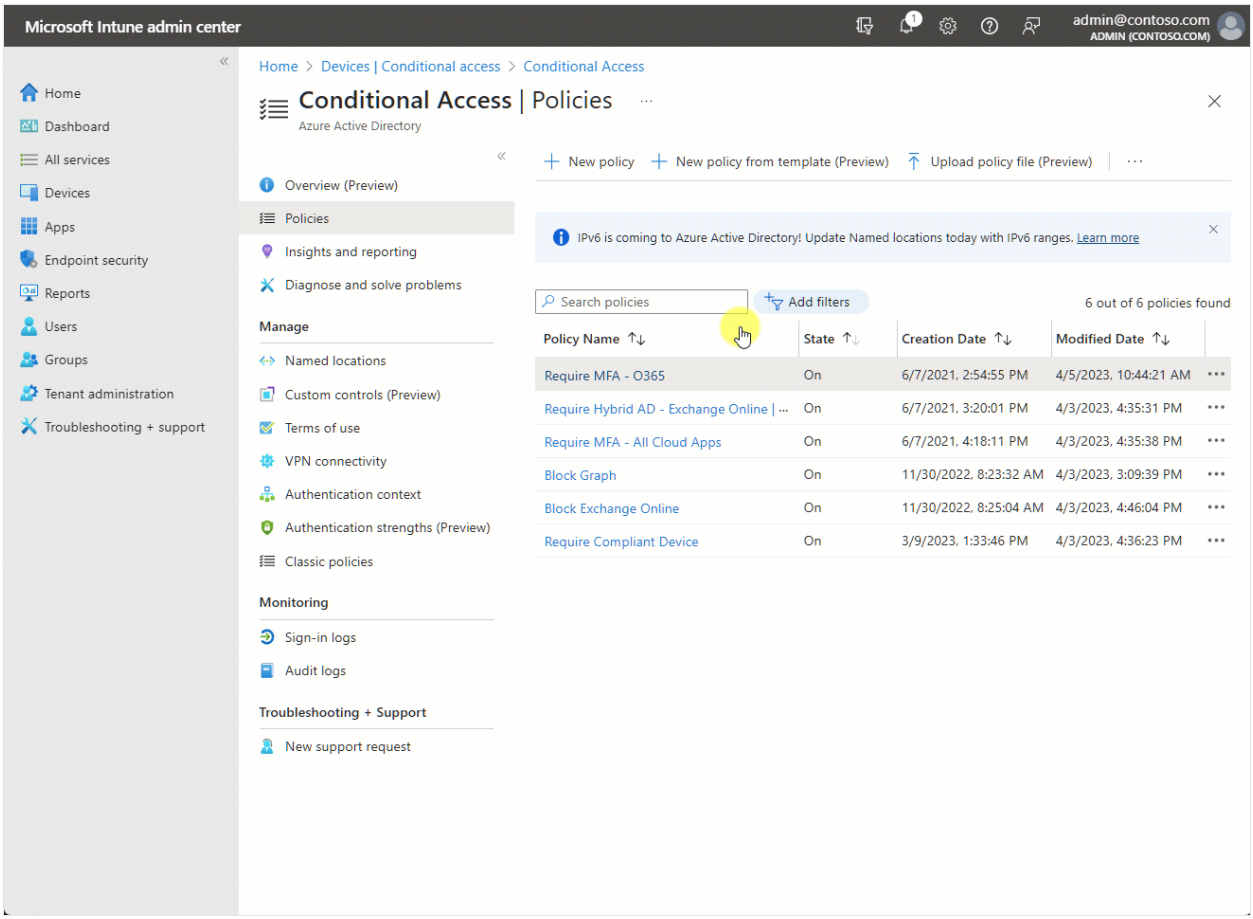
Navigate to your tenant's Conditional Access policies within Endpoint Manager. To access this page, ensure the user has the correct role assigned.

1. Sign into Microsoft Intune admin center
2. Go to **Devices** > **Conditional Access**



Step 2

Select each Conditional Access policy and review its **Assignments** and **Access Controls**. Use the requirements listed above to determine if the policy is compatible with the Surface Hub. If not, the device account needs to be excluded from such policies to sign-in.



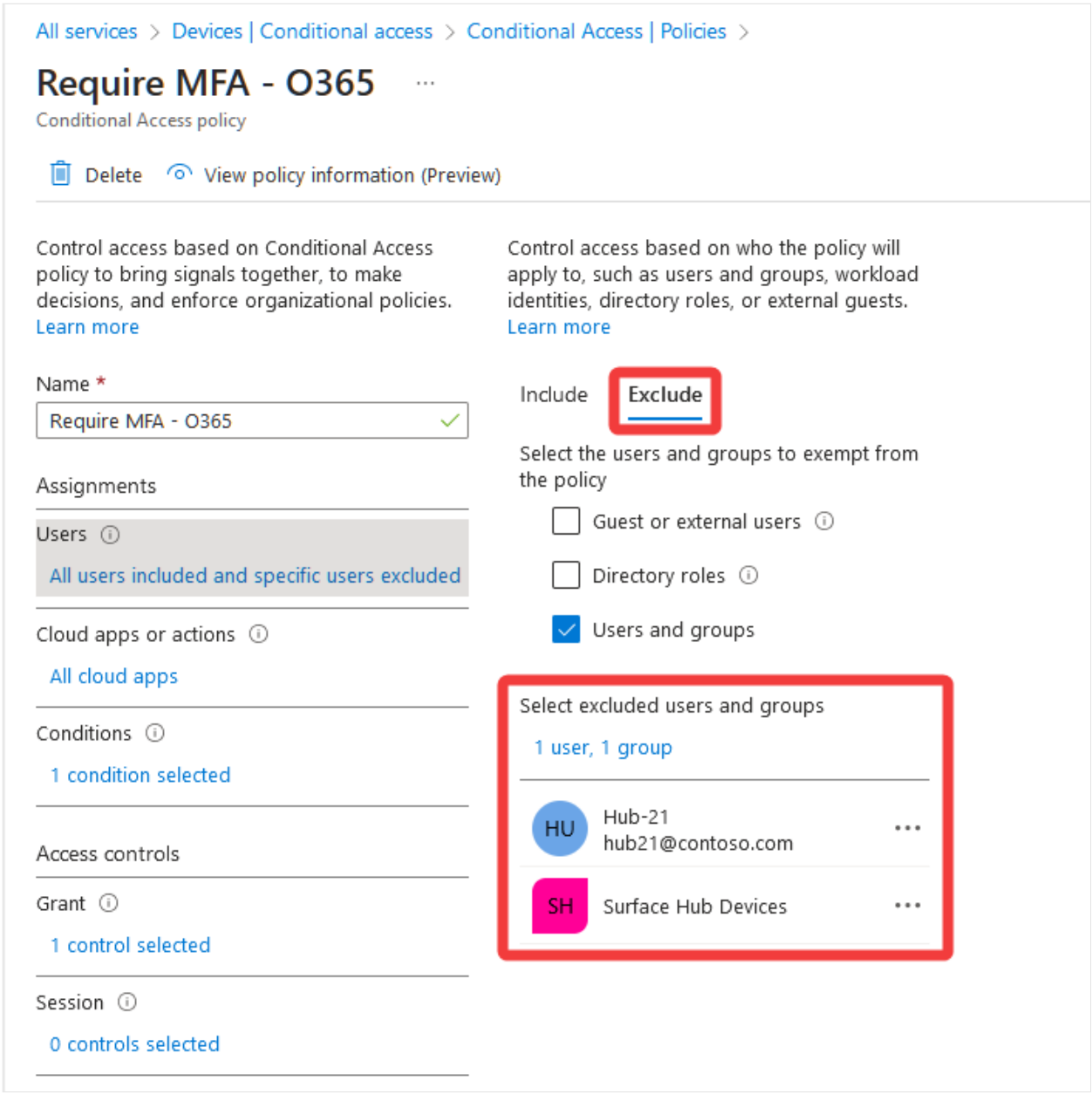
> **Note**
>
> Policies in *On* or *Report Only* states can affect the Surface Hub device account.

Exclude device account from unsupported Conditional Access policies

Due to the limited number of policies the Surface Hub device account supports, it commonly needs to be excluded from Conditional Access policies to allow sign-in. To exclude the device account from a Conditional Access policy do the following:

1. Under Assignments, select **Users** > **Exclude**
2. Select Users and groups
3. Select each individual Surface Hub device account, or group of device accounts.
4. Select Save at the bottom of the screen.

Here's a video demonstrating how to exclude user accounts from a Conditional Access policy.



> **ⓘ Important**
>
> Select the Surface Hub device account **user** object, not the Surface Hub **device** object.

Troubleshoot Intune auto enrollment on Surface Hub

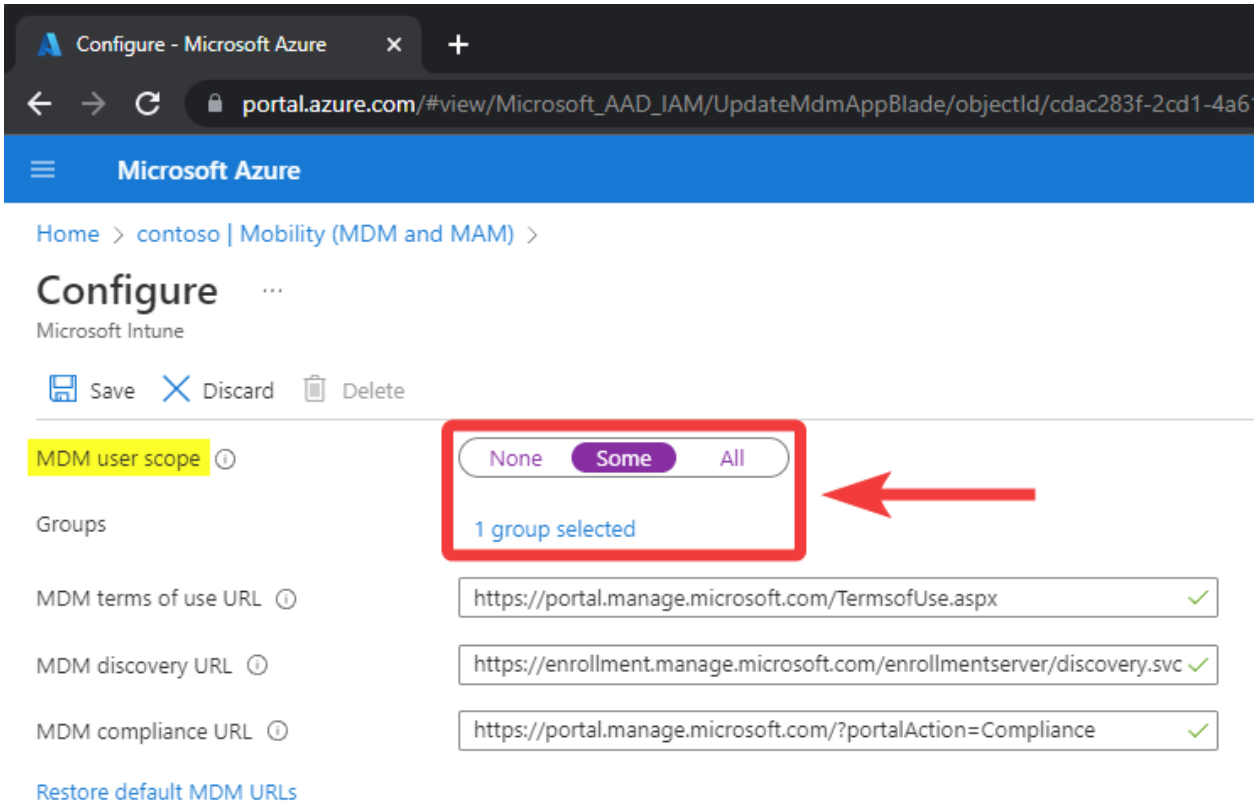
Article • 03/01/2023

If your Surface Hub is joined to Azure AD but fails to automatically enroll in Intune, follow the troubleshooting steps on this page.

Check MDM user scope

Intune auto-enrollment fails when the account used to Azure AD join the Surface Hub wasn't included in the MDM user scope to enroll in Intune. To verify the users and groups included in the MDM user scope:

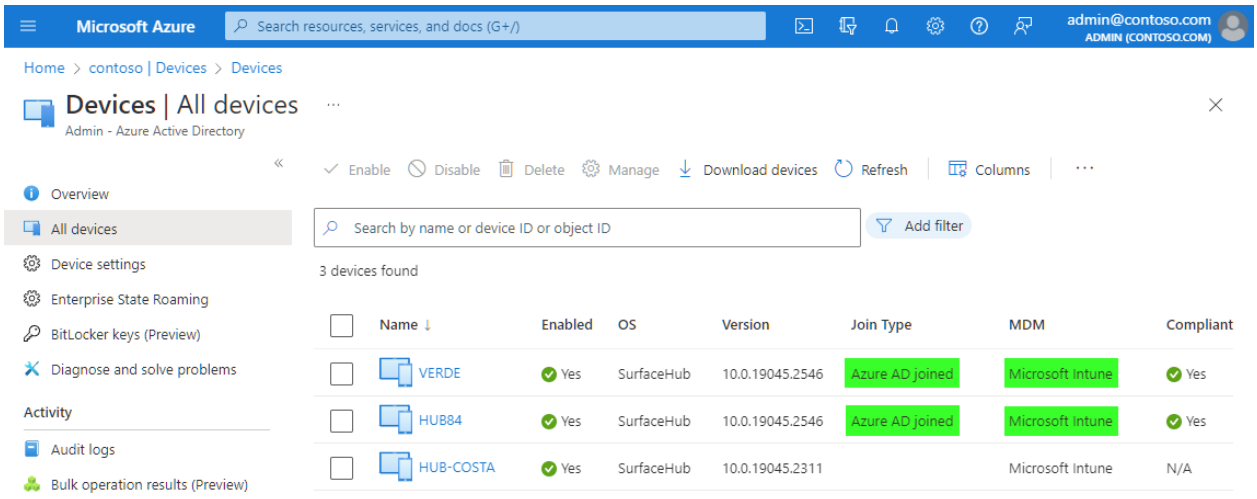
1. Go to the Azure portal, and select **Azure Active Directory** > **Mobility (MDM and MAM)** > **Microsoft Intune.** The MDM user scope section defines the accounts capable of Intune auto-enrollment.
2. Ensure the account used to Azure AD join the Surface Hub is also included in the MDM user scope group. Otherwise, devices don't automatically enroll in Intune during the Azure AD join process.



Identify Intune auto enrolled Surface Hubs

To determine if a Surface Hub was auto-enrolled in Intune:

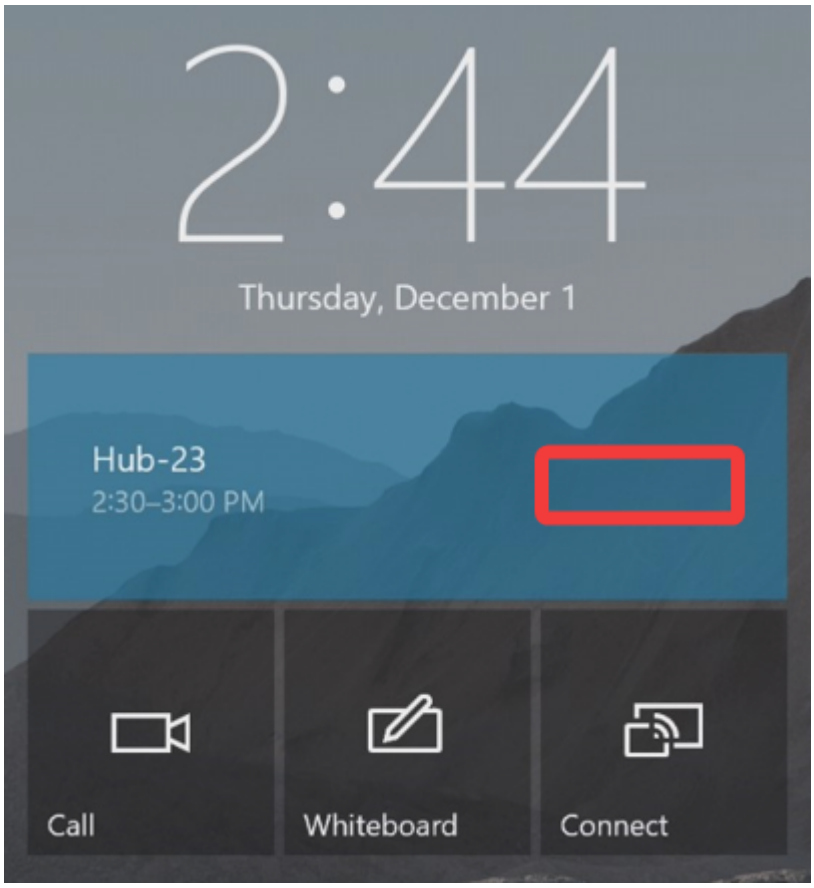
1. Go to the Azure portal and select **Azure Active Directory** > **Devices** > **All Devices.**
2. Locate the Surface Hub and note the join type and MDM fields. If the join type shows "Azure AD joined" with "Microsoft Intune" as the MDM provider, the Surface Hub was successfully auto-enrolled in Intune. If the device lists anything else, it wasn't auto-enrolled in Intune.



Troubleshoot One-click Join from the Welcome Screen calendar

Article • 03/01/2023

When a user invites the Surface Hub to a Teams or Skype for Business meeting, the invitation should appear on the Welcome Screen with a Join button. Tapping the invitation allows the user to join the meeting with one click. If the Join button is missing from the invitation, follow the troubleshooting steps on this page.



How Welcome Screen calendar works

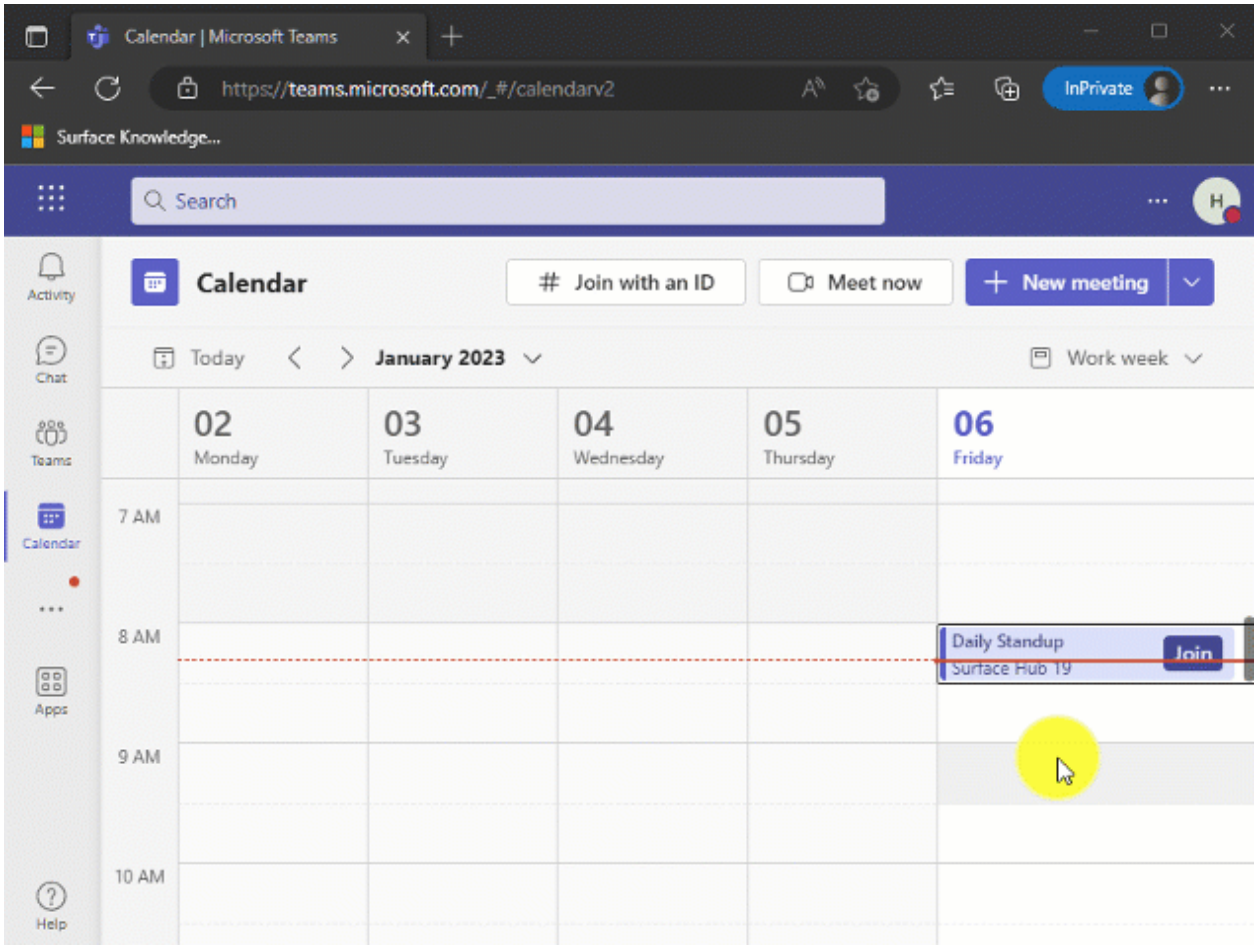
The Welcome Screen calendar parses the meeting join URL from the invitation comments and uses it to join the meeting. If the meeting join URL isn't present in the comments of the invite, the Surface Hub doesn't display the join button.

> **Note**
>
> If the Surface Hub is invited to a Cisco WebEx or Zoom meeting, the Welcome Screen calendar won't display the join button.

Analyze meeting invitation comments

The most common reason you won't see the join button is if the device account's Exchange properties are incorrect, causing Exchange to delete the meeting join URL from the invitation comments. This happens if the device account Exchange property **DeleteComments** is set to **True**. You can confirm if this is happening via the following steps:

1. Open a web browser and navigate to teams.microsoft.com.
2. Sign in with the Surface Hub device account credentials.
3. Open the calendar and locate the Teams meeting that failed to display the join button on the Welcome Screen calendar.
4. Select the meeting and press the expand icon.
5. Below meeting info verify if the Teams meeting join URL is present or not. If missing, follow the PowerShell commands below to check the value of DeleteComments.
6. If the Teams meeting URL is present, analyze the hyperlink to ensure it begins with "https://teams.microsoft.com" and doesn't redirect to a different site. If redirected, the Surface Hub may not understand the URL and therefore not display a join button. Safe Links rewritten URLs, or any other third-party link scanning service isn't compatible with One-click join. Set up a Safe Links policy to exclude the Surface Hub device account from this feature.



Get and set DeleteComments value

PowerShell can be used to verify the current value of DeleteComments, and change it if needed. For Surface Hub to display the join button, DeleteComments must be set to False.

1. Connect to Exchange Online PowerShell.

```PowerShell
Connect-ExchangeOnline
```

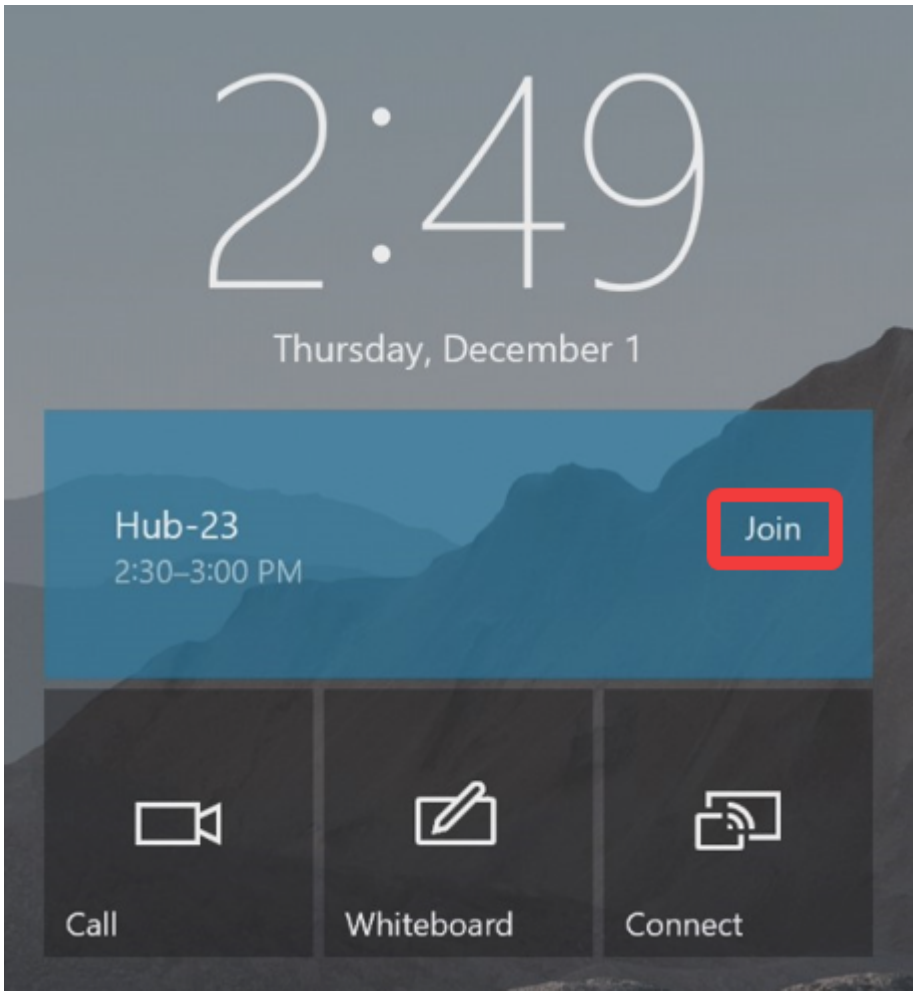
2. This example gets the current value of DeleteComments for account ConferenceRoom01@contoso.com.

```PowerShell
Get-CalendarProcessing -Identity "ConferenceRoom01"  | Select DeleteComments
```

3. If DeleteComments is set to True, change it to False with this command.

```PowerShell
Set-CalendarProcessing -Identity "ConferenceRoom01" -DeleteComments $false
```

After making this change invite the Surface Hub to a new Teams meeting, where the join button should be displayed and allow you to join.


2:49
Thursday, December 1
Hub-23
2:30–3:00 PM
Join
Call
Whiteboard
Connect

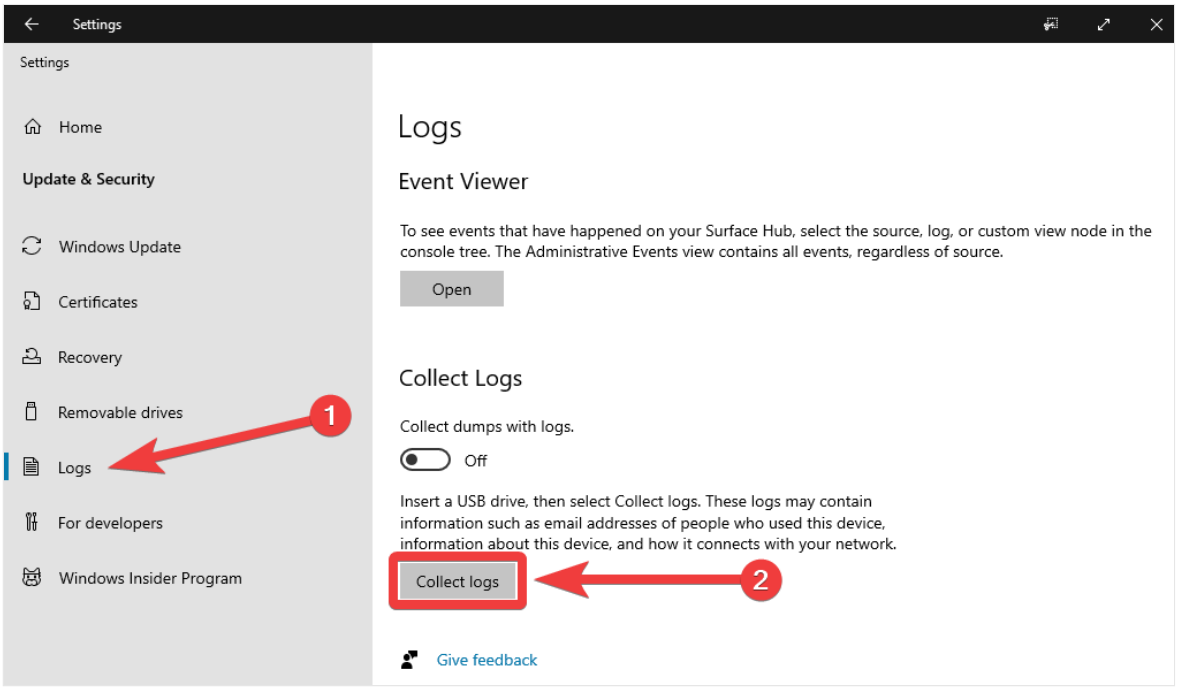
Collect Surface Hub log files

Article • 01/03/2023 • Applies to: Surface Hub, Surface Hub 2S

You can access log files directly from your Surface Hub or remotely via Teams Admin Center.

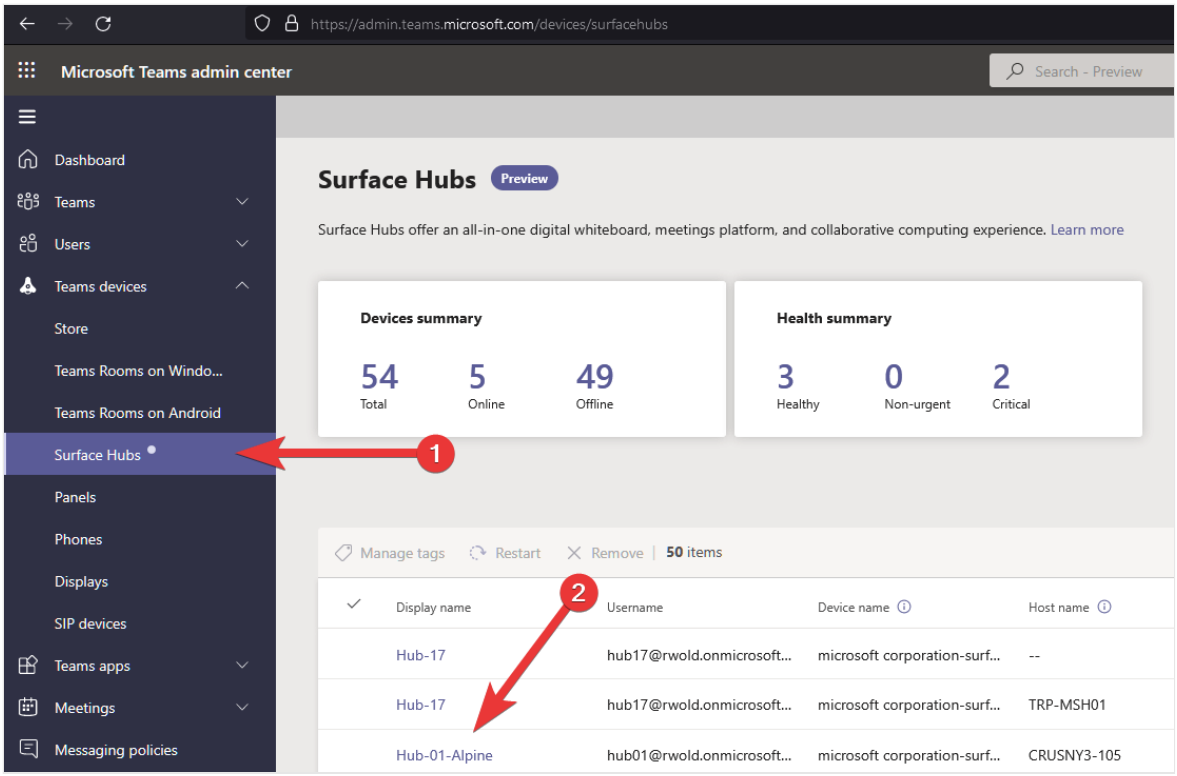
Access logs from Surface Hub

1. Insert a USB flash drive into the Surface.
2. Sign in to Surface Hub with Admin credentials and go to **Settings** > **Update & Security** > **Logs** > **Collect Logs**. This process saves the log files to the root of the USB drive, a process that can take up to 5 minutes.

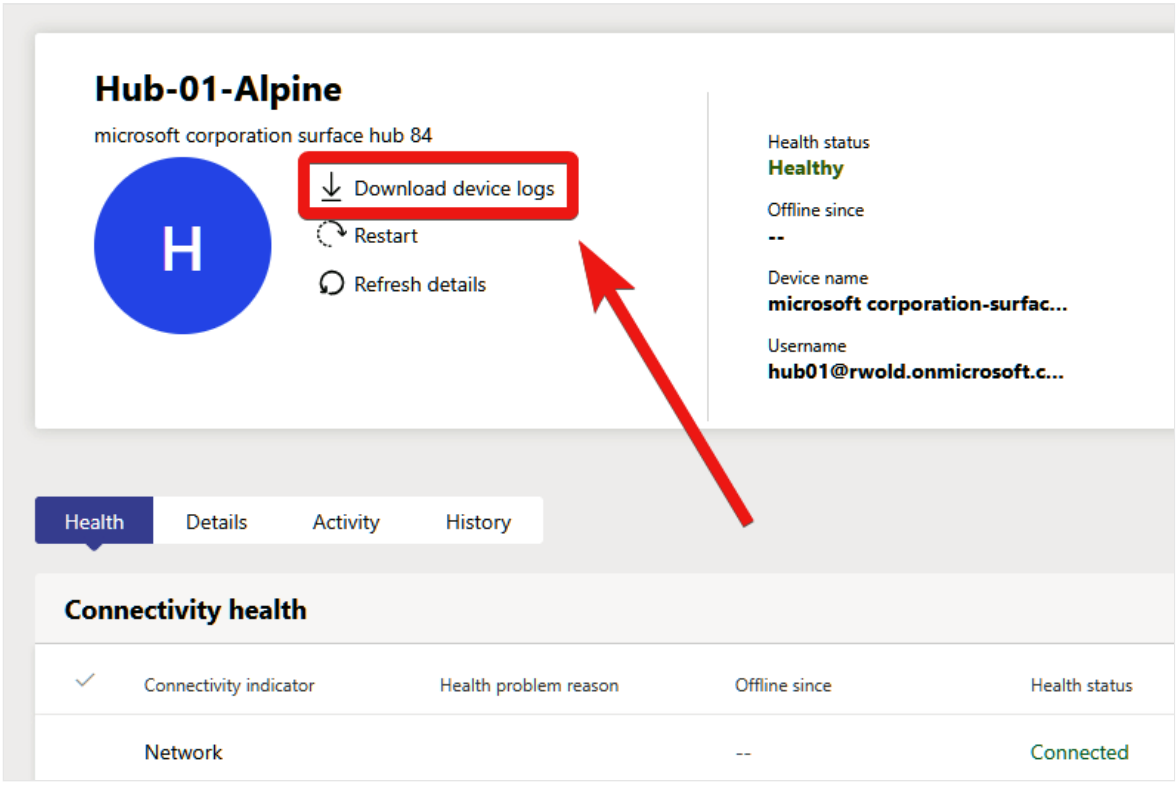


Access logs remotely from Teams Admin Center

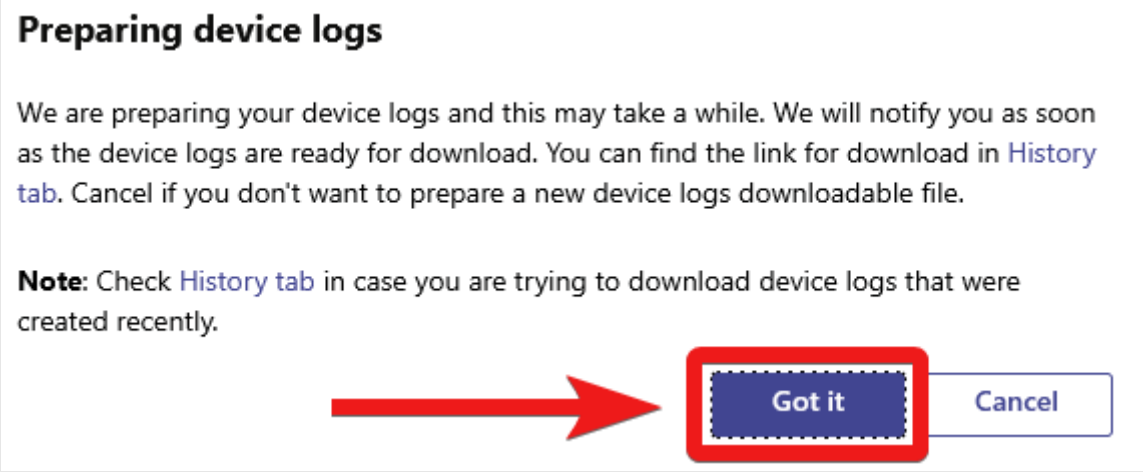
1. Sign in to Teams Admin Center and select **Teams devices** > **Surface Hubs**.
2. Locate your Surface Hub and select its **Display name**.



3. Press **Download device logs**.

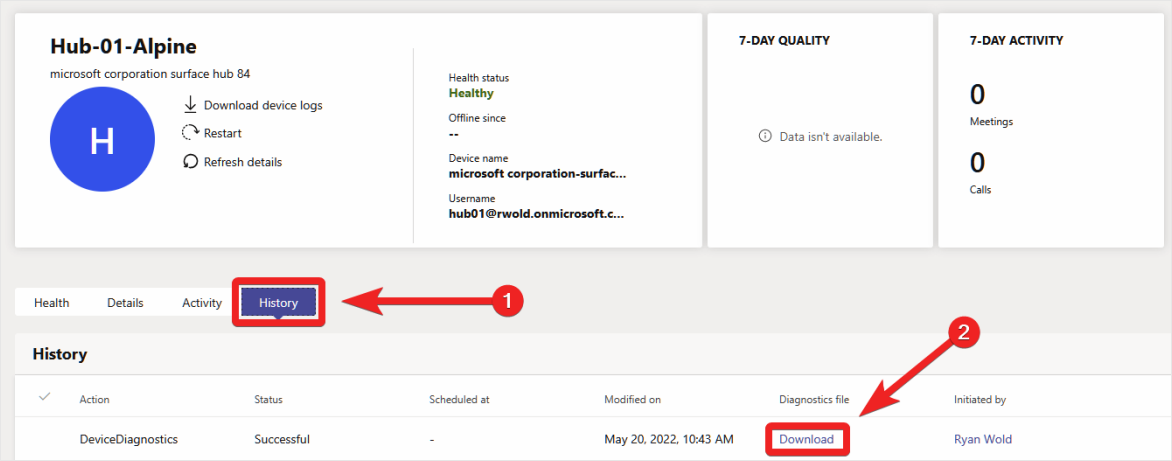


4. Press **Got it** to prepare the device logs for download.



5. Select the **History** tab to view the status of the log collection process and download the logs when they're available.

6. When the logs are ready, press **Download**. This process saves the log files to the Downloads folder on your PC.



Learn more

- What's new in Windows 10 Team 2020 updates
- Windows Event Viewer

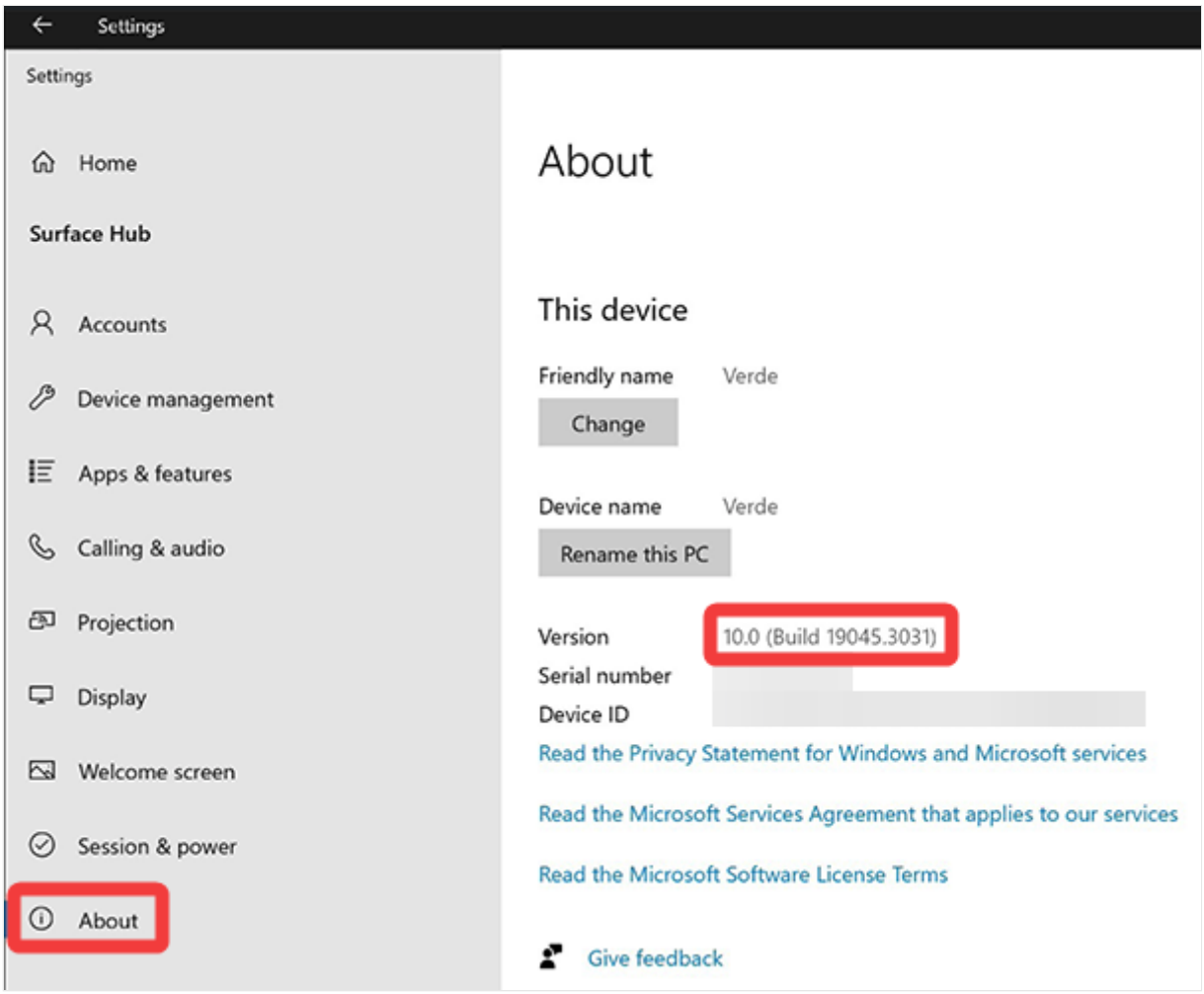
Troubleshoot Surface Hub not Updating

Article • 06/28/2023

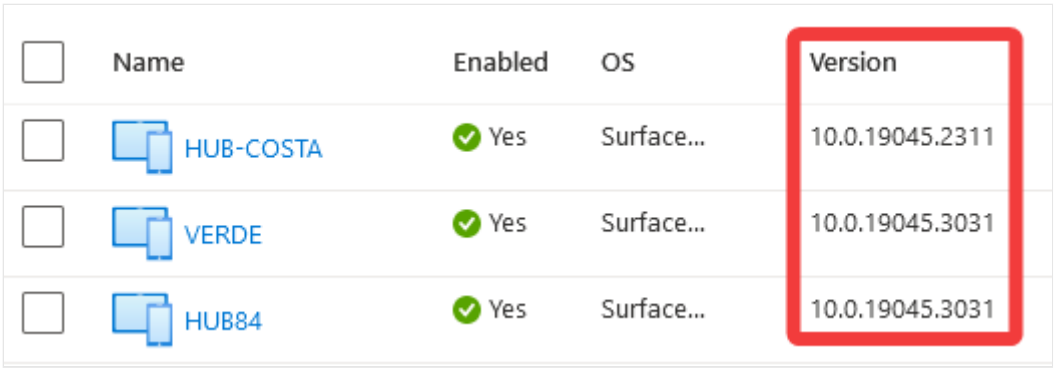
If your Surface Hub isn't automatically installing Windows Updates, follow the troubleshooting steps on this page.

Verify current Surface Hub build number

First, determine the OS build number the Surface Hub is currently running. You can do this in-person via **Settings** > **Surface Hub** > **About**.



If the Surface Hub is Azure AD joined, you can verify the OS build number by navigating to the Azure portal, Select **Devices** > **All Devices** and locate the Surface Hub.



Compare the OS build number the Surface Hub is running with the Surface Hub update history page to see which updates are missing. The current Surface Hub OS version is Windows 10 Team 2022 Update (22H2 / 19045). More details on how to do this are covered in the verify a Surface Hub is fully updated video.

Network requirements and troubleshooting

If your organization uses a proxy or firewall, ensure the necessary connection endpoints for Windows 10 Enterprise and Windows Updates endpoints are accessible by the Surface Hub.

Proxy server

If you have a proxy server configured and Windows updates either don't download or remain stuck at 1% progress, it can be caused by the following:

- SSL inspection
- Cache updates from Windows Update
- Block support for partial file download (HTTP range headers)

Windows update uses dynamically created temporary file names that differ for each computer that downloads updates. This eliminates any benefit that might be gained from caching. Windows update also uses the Background Intelligent Transfer Service (BITS) as a client, which can request partial files, an operation the proxy may not support.

To resolve this issue, ensure the proxy doesn't perform any of the above operations on Windows Update traffic. More requirements and information can be found in Windows Update issues troubleshooting.

If you're using a Bluecoat proxy, you can find more details at Microsoft Windows updates fail to install.

> **Third-party information disclaimer**

> Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

Test with open network

For troubleshooting purposes you can test connecting the Surface Hub to an open network to see if the device is able to download Windows updates. This will help confirm if the internal network isn't meeting the necessary network requirements for Windows update. To test with an open network do the following:

- If a proxy is configured, unconfigure it on the Surface Hub. **Settings** > **Network & internet** > **Proxy**
- Disconnect the Surface Hub from the network and connect it to a mobile Wi-Fi hotspot. **Settings** > **Network & internet** > **Wi-Fi**
- Navigate to **Settings** > **Update & security** and check for updates. If updates are still not found reboot the device and try again.

Mirror network port

Port mirroring is a technique used on a network switch or router to send a copy of network packets seen on the specified ports (source ports) to other specified ports (destination ports). After enabling port mirroring on the Surface Hub port, the packets can be monitored and analyzed by an administrator to determine if any Microsoft endpoints are unaccessible.

Windows Update for Business deferral policy

Windows Update for Business is a feature that allows IT administrators to manage when Windows devices receive updates. Administrators can defer or pause updates, allowing time to validate them before installing them on all devices. Feature updates can be deferred up to 365 days and quality updates can be deferred up to 30 days. Deferring means the device won't receive the update until it has been released for at least the number of deferral days you specified (offer date = release date + deferral date).

If your Surface Hub isn't updating, confirm if a Windows Update deferral policy is applied. The specific policies are:

- Update/DeferFeatureUpdatesPeriodInDays
- Update/DeferQualityUpdatesPeriodInDays

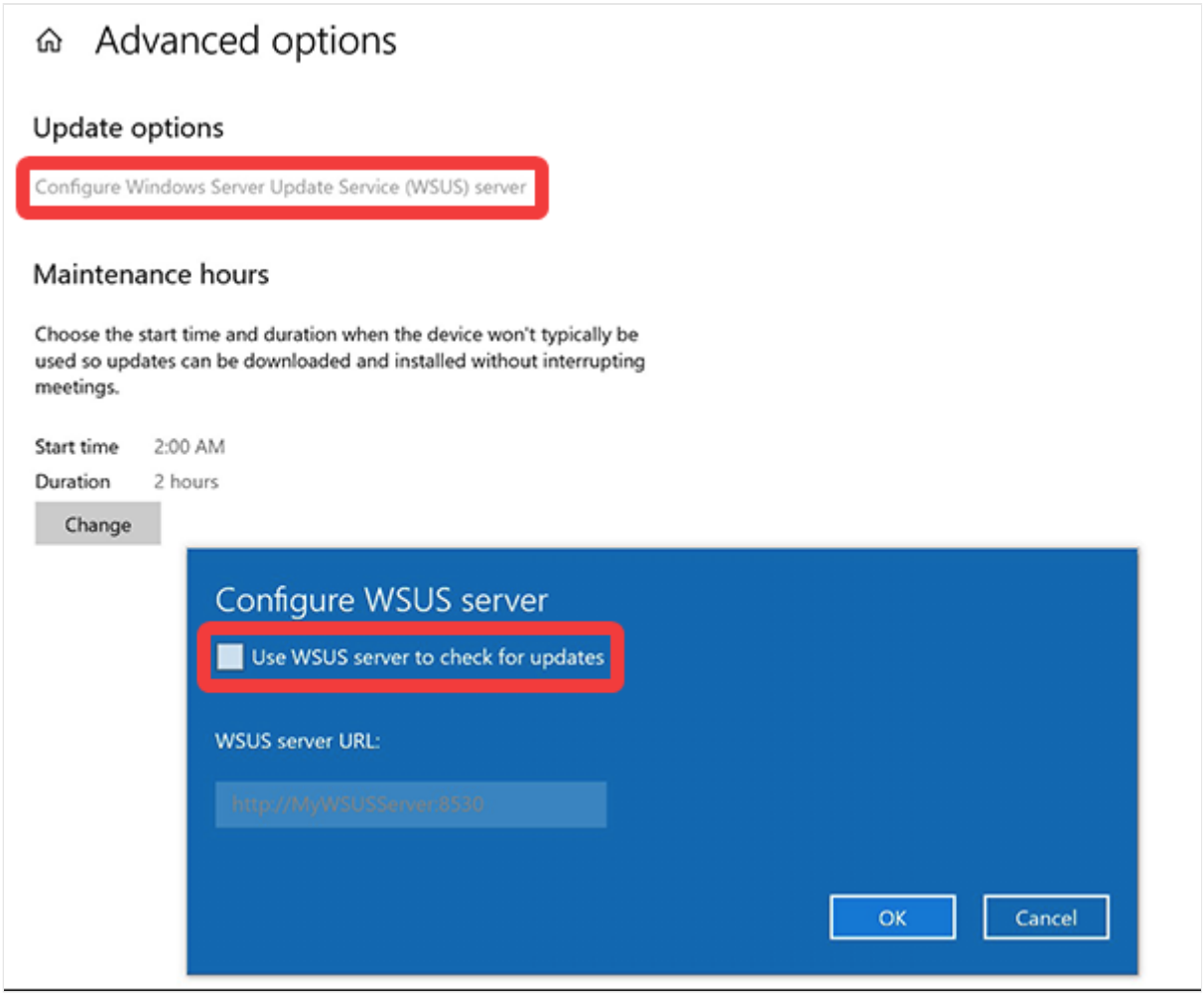
Surface Hub v1 devices not updating past Windows 10 Team version 1703 (15063)

In some environments, Surface Hub v1 devices fail to install updates past OS build number 15063. If you have a Surface Hub experiencing this, the device needs to be reimaged using the Surface Hub Recovery Tool.

Confirm WSUS isn't configured

The Surface Hub no longer supports Windows Server Update Services (WSUS). If the Surface Hub is configured to use WSUS, Windows Updates won't be received. Confirm WSUS isn't configured on the device by going to **Settings** > **Update & security** > **Windows Updates** > **Advanced options** > **Configure Windows Server Update Service (WSUS) server**.

Ensure "Use WSUS server to check for updates" is **unchecked**.

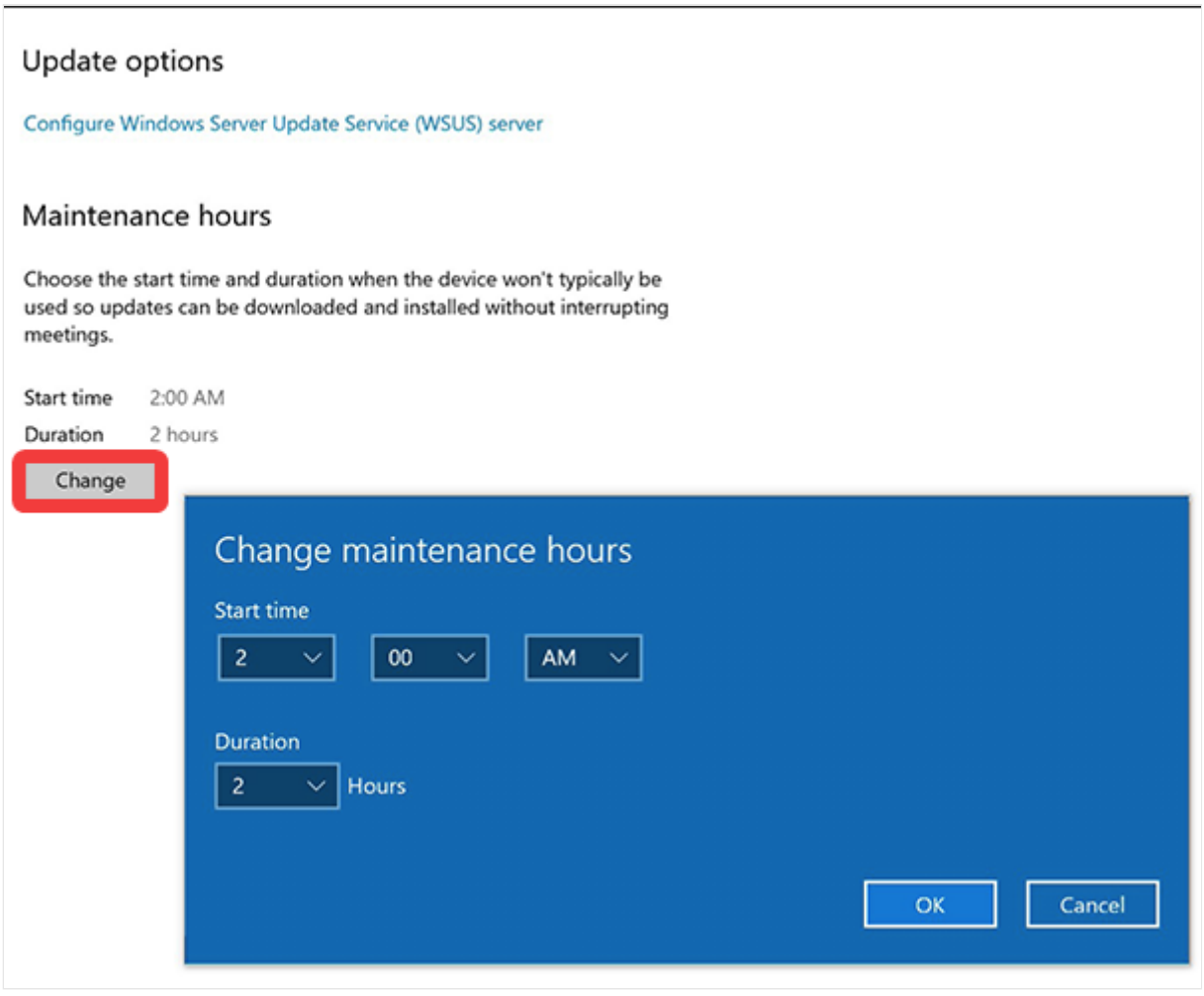


Surface Hub not performing nightly maintenance

The Surface Hub automatically installs Windows Updates during the nightly maintenance window. The default maintenance window is set to begin at 2:00 AM for two hours. If the Surface Hub is unable to perform maintenance, it can result in the device not installing Windows updates. Common reasons for this include:

- The device is unplugged or powered off
- Surface Hub is reserved for a 24 hour interval meeting
- Device is in use during the maintenance window

We recommend you refrain from using or reserving the Surface Hub during the scheduled maintenance period. You can adjust the maintenance window timeframe by opening **Settings** > **Update & security** > **Windows Update** > **Advanced options**. Selecting "Change" allows you to adjust the maintenance hours. A maintenance window of at least 2 hours should be reserved for update.

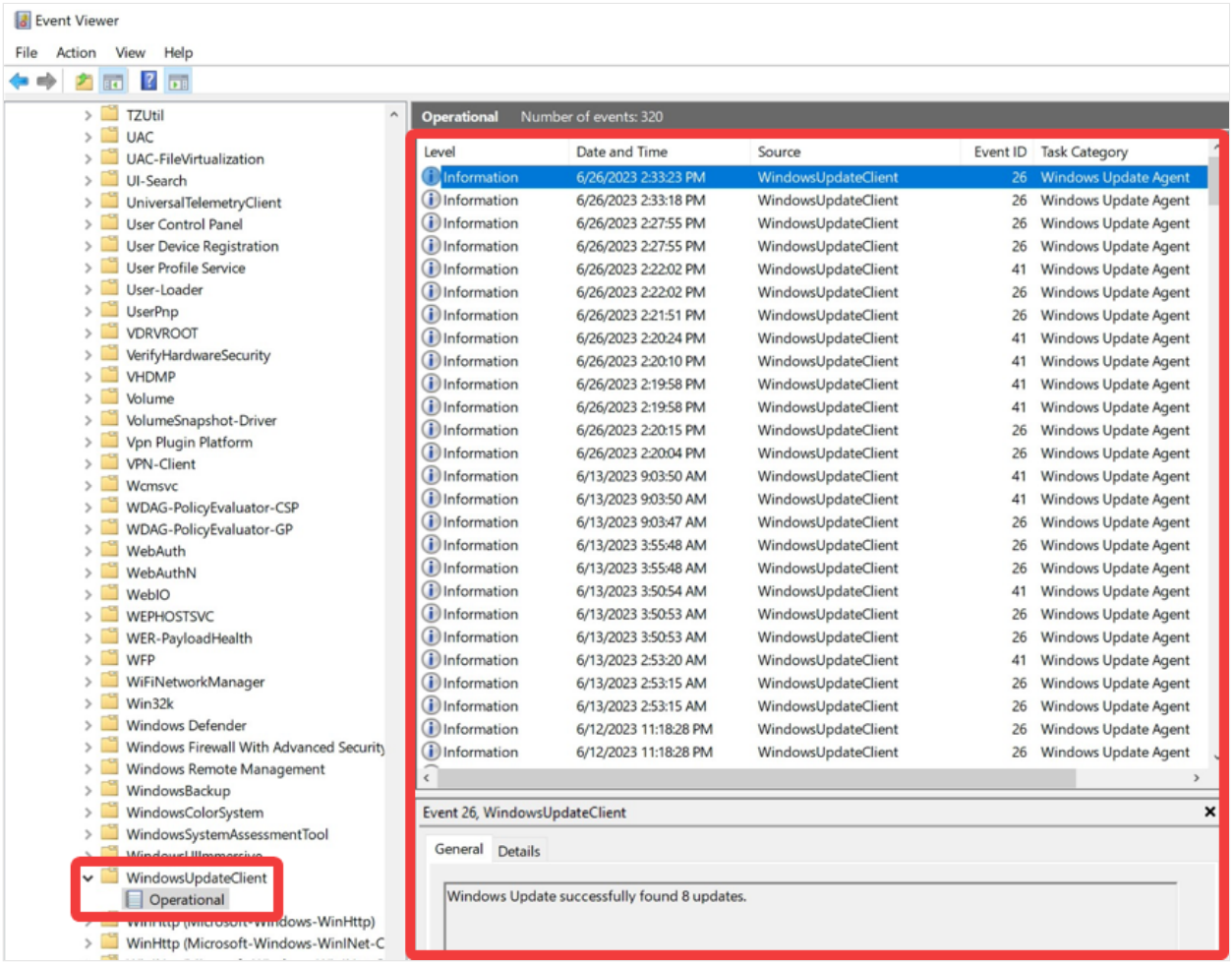


Windows event logs

You can view the Windows Event logs on the Surface Hub to see if any errors are present.

On the Surface Hub navigate to **Settings** > **Update & security** > **Logs** > **Event Viewer** > **Open.**

Windows Update event logs can be found under **Applications and Services Logs** > **Microsoft** > **Windows** > **WindowsUpdateClient** > **Operational.**



Reimage Surface Hub

If the troubleshooting steps in this article don't resolve the Surface Hub updating issue, the local Windows Update cache on the device may be corrupt. The device needs to be reset to resolve this issue. Detailed instructions on resetting the device can be found in the articles for Surface Hub v1 and Surface Hub 2S.

Troubleshoot Teams sign-in issues on Surface Hub

Article • 01/25/2023

If you can't sign in to Microsoft Teams on Surface Hub, several recommended troubleshooting steps are described on this page.

- First, make sure your Surface Hub is running the latest updates. To learn more, see the following video: How to verify a Surface Hub is fully updated .
- Check Microsoft Teams is updated to the latest version. On Surface Hub, open **Microsoft Teams**, select **...** > **Settings** > **Check for updates**.
- Use the Azure sign-in logs for insights into sign-in errors. You can filter by the Surface Hub device account and look for any failures.
- If you still can't sign in, look for the error code displayed on the Teams sign-in screen and review the following table for troubleshooting steps and links to relevant documentation.

Error codes	Possible root cause	How to resolve	Learn more
CAA20003	Incorrect time on device	Ensure KB5011543 or a newer Windows update is installed (build 19042.1682 or later).	- Video: How to verify a Surface Hub is fully updated - Manage Windows updates on Surface Hub

Error codes	Possible root cause	How to resolve	Learn more
	Conditional Access (CA) Policy	A device account can't have CA enabled. To resolve this issue, ensure your Surface Hub device account is excluded from any CA policies. 1. Begin with the Azure AD conditional access What If tool to see which policies currently apply to your device account. 2. Run the tool in Report-only mode, which lets you evaluate the impact of Conditional Access policies before enabling them in their environment.	- Troubleshooting sign-in problems with Conditional Access - Troubleshoot Conditional Access using the What If tool - What is Conditional Access report-only mode? - Video: Use the Report Only feature to test Conditional Access policies
CAA90014	Device account password expired	1. Open Microsoft Edge and attempt to sign in to Microsoft 365 with your device account credentials. 2. If prompted to change the device account password, go ahead and change it. 3. On Surface Hub, go to **Settings** > **Surface Hub** > **Accounts**> **Device account** > **Change**. 4. Select **Start over with a new device account**. The current device account will be removed when you set up a new one using your new credentials.	- Password management (Surface Hub)
	Incorrect time on device	Ensure KB5011543 or a newer Windows update is installed (build 19042.1682 or later).	- Video: How to verify a Surface Hub is fully updated - Manage Windows updates on Surface Hub

Error codes	Possible root cause	How to resolve	Learn more
	Multi-Factor Authentication (MFA)	A device account can't have MFA enabled. To resolve this issue, try excluding the Surface Hub device account from MFA and test again.	- Create and test a device account
CAA10001 or AUTH0006	Conditional Access (CA) Policy	Follow the instructions above to resolve Conditional Access issues.	
	No device account added	To confirm a device account is added: 1. On Surface Hub, go to **Settings** > **Surface Hub** > **Accounts**. 2. Verify that a device account is added successfully: A device account will show as **Not Set** if it isn't added. 3. Create and add a device account and try connecting to Teams again.	- Create and test a device account
unknownautherror	Hub still running earlier OS	Surface Hub v1 only: 1. Ensure the device is updated to Windows 10 Team 2020 Update (20H2). 2. If your Hub v1 device is still running an earlier OS, it could be affected by the following known issue: **A small subset of v1 Surface Hub devices is not able to automatically upgrade to the Windows 10 Team 2020** 3. To resolve, reimage Hub v1 using the Surface Hub Recovery Tool and upgrade to 20H2.	- Known issues: Surface Hub - Using the Surface Hub Recovery Tool
	Conditional Access (CA) Policy	Follow the instructions above to resolve Conditional Access issues.	

Support requests

If you still can't successfully sign in to Teams, you can create a support request. Include the following items:

- Any error codes displayed when you attempt to sign in to Teams.
- Log files, as noted below.

Diagnostic Teams log files

When creating a support request with Microsoft Support, the support engineer will require diagnostic log files. Having the logs before creating the support request will allow Microsoft to quickly start troubleshooting the problem.

To collect Teams log files:

1. Connect an external keyboard to Surface Hub.
2. Open the Teams app and reproduce the issue by attempting to sign in.
3. Select the Teams app and ensure the focus is on Teams as the active app on the Hub display.
4. On your keyboard, press **Tab** three times to highlight the UI element for settings, represented by three dots (**...**).
5. Press **CTRL + ALT + SHIFT + 1** to download the Teams log files.
6. Open **File Explorer**, go to **Downloads**, and look for the folder containing the Teams log files.
7. Copy the folder to a USB drive.

To learn more, see Configure log files for monitoring and troubleshooting in Teams

Surface Hub & Azure log files

- Surface Hub log files
- Any applicable Azure sign-in logs that indicate sign-in failure

Troubleshoot access to Settings app on Surface Hub

Article • 01/10/2023

To open the Settings app on Surface Hub, select **All apps** > **Settings**. Note that Ease of Access settings are available to anyone using Surface Hub. For all other settings, select **View as Admin** and log in with an Admin account. If you're unable to access settings after attempting to log in with your Admin account, review the troubleshooting guidance on this page, beginning with Device affiliation.

Device affiliation

Full access to the Settings app on Surface Hub depends on how you initially affiliated Surface Hub during first run setup (aka OOBE) via one of the following options:

- Azure Active Directory (AAD)
- On-premises AD (Active Directory)
- Local account administrator

Azure Active Directory (AAD)

By default, when Surface Hub is joined to AAD, only an account designated as a Global Administrator (GA) in your Azure tenant can access Settings. If unable to access Settings, check the following issues:

- Is the account a Global Admin account?
- Is the password expired? Try resetting the password.
- Is Surface Hub connected to the internet?
- Is Surface Hub behind a proxy or firewall that blocks access to AAD?
- Did you or another admin configure non-Global Admin policy for Surface Hub? If yes, see the following section.

Troubleshoot non-Global Admin policy

When joined to AAD and auto-enrolled in Intune, you can configure non-Global Admin policy to allow other accounts to access Setting on Surface Hub. If non-Global Admin policy is enabled and users cannot access Settings, check the following issues:

Policy succeeds: Still no access to Settings

If Intune shows the non-Global Admin policy setting is successfully applied to Surface Hub:

- Is the account attempting to log in a member of the security group designated for this policy?
- Is the Surface Hub connected to the internet?
- If a GA account is being used, is it a member of the security group configured on the Surface Hub? GA accounts must also be added to this security group. Otherwise, if non-Global Admin policy is applied to Surface Hub, the GA can no longer access Settings.

Policy fails: Intune error

If Intune shows the non-Global Admin policy setting fails to reach Surface Hub:

- Is the security group for the accounts created in the cloud?
- Is the correct Azure AD group SID (security identifiers) used in the XML?
- Is the XML file created correctly?
- Ensure the policy is assigned to Surface Hub device objects, not the device accounts.

To learn more, see Troubleshoot policies and configuration profiles in Microsoft Intune

On-premises AD

If the Surface Hub is domain joined and connected to on-prem AD, a security group in AD is specified during first-run setup to allow group members to sign into Settings. This designated group can be seen on Surface Hub within Settings > Surface Hub > Accounts. If an error message is received stating “this requires elevation” when attempting to log into Settings, check the following issues:

- Ensure the account being used is a member of the security group designated during OOBE.
- Ensure the account is enabled and the password has not expired.

> ⓘ **Note**
>
> If the Surface Hub loses trust with the domain and Settings can no longer be accessed, you will need to reset Surface Hub.

Local admin - no device affiliation

If you choose to set up Surface Hub with a local admin (no device affiliation to AAD or on-prem AD), the account created during first run setup is the only account that can access Settings. The local admin account is not backed by any directory service. If the credentials are forgotten or no longer working, you will need to reset Surface Hub.

> **ⓘ Important**
>
> If the local admin account was created using a **provisioning package**, the password must be reset every 42 days. Otherwise, the account may be locked out and unable to sign into Settings. If this occurs, you will need to reset Surface Hub.

Learn more

- Reset and recovery for Surface Hub 2S
- Reset and recovery for Surface Hub v1

Troubleshoot configuration service provider policy settings for Surface Hub

Article • 02/06/2023

Configuration service providers (CSPs) enable a rich set of options for deploying policy settings to Surface Hub. Try these common troubleshooting steps if your CSP settings are not working on your Surface Hub.

1. First, ensure that Surface Hub is enrolled in a mobile device management (MDM) provider--without errors and is syncing correctly. To verify, sign in to Surface Hub with an admin account, and go to **Settings** > **Surface Hub** > **Device management**. If you see a tenant with an email address, the device is enrolled in MDM.

2. To check the sync status or any sync errors, select the email address and choose Info to display the device sync status.

Troubleshoot MDM issues

1. Refer to the following documentation to verify that your CSP is supported on Surface Hub.

    - SurfaceHub CSP
    - CSPs supported in Microsoft Surface Hub
    - Policies in Policy CSP supported by Microsoft Surface Hub

2. Upon confirmation that your CSP is supported on Surface Hub, sign in to the Endpoint Manager Admin Center. Choose **Devices** > **Configuration profiles** and select your CSP.

3. On the CSP page, ensure the **Configuration profile** is applied to a **Device group** (not a user group or device account).

4. Ensure your CSP is successfully deployed to your Surface Hub. In Endpoint Manager, select **Devices** > **All devices** > and choose your Surface Hub.

5. Select **Device configuration** and check that the CSP is deployed successfully.

6. Ensure the appropriate Intune URLs/IP ranges are allowed through the proxy/firewall.

Troubleshoot display projection to Surface Hub

Article • 02/16/2023

Surface Hub is designed to enable end users to project their display from laptops or other external devices wirelessly via Miracast or via wired (USB-C/HDMI) connections. Surface Hub listens for incoming wireless connections via Miracast when Wi-Fi is enabled. If your external device supports Miracast and runs Windows 10 or Windows 11, you should be able to wirelessly project your screen onto Surface Hub. If you can't, try the troubleshooting steps on this page.

To connect with Miracast:

1. On your Windows 10/11 device, press **the Windows logo key + K**.
2. In the **Connect** window, look for the name of your Surface Hub in the list of nearby devices, as shown in the bottom left corner of the Surface Hub display.
3. Enter a PIN if your system administrator has enabled the PIN setting for Miracast connections. This requires you to enter a PIN when you connect to Surface Hub for the first time.

> **Tip**
>
> If you don’t see the name of the Surface Hub device as expected, it's possible the previous session was prematurely closed. If so, sign in to Surface Hub directly to end the previous session and connect from your external device.

Troubleshoot Miracast

Table 1. Troubleshoot Miracast connections to Surface Hub

Action	Where	Notes
Restart devices	External device/Surface Hub	If Miracast has worked previously, restart your external device or restart your external device and Surface Hub to reset the connection.
Restart wireless display adapter	External device	1. **Start** > **Settings** > Bluetooth **& devices** > **Devices**. Under **Wireless displays & docks**, select the wireless display or adapter. 2. Select **Remove device** > **Yes**. 3. Try reconnecting.

Action	Where	Notes
Check Wi-Fi is turned on	Surface Hub	- Open **Settings** > **View as Admin**. Select **Network & Internet** and make sure **Wi-Fi** is turned **On**. **Note**: Surface Hub doesn't need to be connected to a wireless network, but Wi-Fi must be enabled for Miracast to work.
Verify Miracast projection is turned on	Surface Hub	1. Open **Settings** > **View as Admin**. Select Surface Hub> Projection. 2. Make sure the following settings are turned on: - **Connect automatically when someone projects** - **Presenters can use Miracast to protect wirelessly to this device** **Note:** If a PIN is required, users must enter it when they connect an external device for the first time.
Verify Miracast support	External device	1. Press **Windows logo key** + **R** and type **dxdiag**. 2. Select **Save all information.** 3. Open the saved **dxdiag.txt** file and find **Miracast**. It should indicate **Available, with HDCP**.
Check Miracast channel	Surface Hub	If you run a network scan, you should see Surface Hub Miracast listed as an access point. If Surface Hub's Miracast network appears, but you can't see it as an available device, try to adjust the Miracast channel. When Surface Hub is connected to a Wi-Fi network, it uses 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'll need to restart Surface Hub after each change. Use channels that don't show heavy utilization from the network scan.
Check drivers	External device	Ensure the device drivers on your external device are up to date and the latest firmware is installed for your wireless display or adapter. In **Device Manager**, select **Network Adapters**, open the Wi-Fi adapter and video adapter and check for an updated driver version.
Check firewall	External device	The Windows firewall can block Miracast traffic. The most straightforward 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.

Action	Where	Notes
Check Group Policy settings	External device (domain joined)	On domain-joined devices only, Group Policy can also block Miracast. 1. Press **Windows Key + R** and type **rsop.msc.** The **Resultant Set of Policy** snap-in shows the current policy settings applied to the PC. 2. Review **Computer Configuration** > **Windows Settings** > **Security Settings** > **Wireless Network (IEEE 802.11) Policies**. There should be a setting for wireless policies. 3. Double-click the setting for wireless policies, and a dialog box appears. 4. Open the **Network Permissions** tab and select **Allow everyone to create all user profiles**.
Check Event logs	External device/Surface Hub	The last place to check is in the Event logs. Miracast events are logged to **Wlanautoconfig** on both Surface Hub and the external device. If you export Surface Hub logs, you can view Surface Hub's Wlanautoconfig in the **WindowsEventLog** folder. The event log errors can provide more details on where the connection fails.

Troubleshoot connection performance

After wireless projection is connected, it's 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 use channels with less traffic.

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

If Surface Hub and the projecting device are connected to Wi-Fi but use different access points with different channels, forced channel switching degrades performance when Miracast is connected. The channel switching affects 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 Surface Hub's channel 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. Some channel switching is unavoidable if there are multiple Wi-Fi networks or access points in the environment. In this scenario, ensure all Wi-Fi drivers are up to date.

Surface Hub Miracast channels 149-165 not supported in Europe, Japan, Israel

In compliance with regional governmental regulations, all 5-GHz wireless devices in Europe, Japan, and Israel don't support the Unlicensed National Information Infrastructure-3 (U-NII-3) band. In Surface Hub, the channels associated with U-NII-3 are 149 through 165. This includes Miracast connections on these channels. Therefore, Surface Hubs used in Europe, Japan, and Israel can't use channels 149-165 for Miracast connections.

Troubleshoot wired connections

- Device resolution not supported error
- Connect app exits unexpectedly

Device resolution not supported error

When you try to project from a Surface Pro, Surface Book, or Surface Laptop to an 84-inch Surface Hub by using the HDMI port on the Surface Hub, the error message "Device Resolution isn't supported" is displayed.

- **Cause:** The Surface device isn't set to a supported 84" ingest resolution. By default, Windows tries to connect to the Surface Hub using *Duplicate* mode, duplicating your desktop on both screens. But the default resolution of the Surface device is higher than the 1080-p resolution of the Surface Hub, so the Hub can't display the higher-resolution image.
- **Resolution:** Projecting to a second screen can be accomplished by using *Extend*. Extend is used to expand the desktop user interface across your Surface and Surface Hub displays, allowing each to display the desktop in its native resolution. Use one of the following methods to configure your Surface to display your desktop in Extend mode.

Method 1: Change the desktop resolution

1. Open **Start**, and then select **Settings** > **System** > **Display**.
2. Select the Surface Hub display from the choice made available.
3. Under **Scale and layout**, change the setting under **Resolution** to **1920 x 1080**.

Method 2: Change Project setting to Extend

- Press **Windows key+P** and then select **Extend**.

Connect app exits unexpectedly

At times, a wired Connect session that is started from the Welcome screen by connecting a DisplayPort input will exit back to the Welcome screen after using the side keypad or the source button to cycle through all source inputs.

- **Cause:** This is an issue in the Connect app and its default full-screen state. By changing the size of the app or by selecting a DisplayPort input thumbnail in the Connect app, you can prevent input cycling from affecting the app.
- **Resolution:** Launch the Connect app from the Welcome screen and connect a DisplayPort input to resolve this issue. If the input is already connected, manually select the thumbnail.

Contact Support

If you have questions or need help, you can create a support request.

Learn more

- Connect devices to Surface Hub 2S
- Connect other devices and display with Surface Hub v1

Surface Hub can't download updates from Windows Update

Article • 05/11/2023

This article helps resolve the issue in which Surface Hub can't download updates from Windows Update. The download either doesn't start or remains stuck at 1% progress.

Applies to: Surface Hub
Original KB number: 3191418

Symptoms

If you have a proxy server configured and you try to check for and download updates through Windows Update on the Surface Hub, the download either doesn't start or remains stuck at 1% progress. If you check for and download updates on a connection that has a direct access to the Windows Update servers, this works without a problem.

Cause

This issue occurs if a proxy tries to do any of the following:

- SSL inspection
- Cache updates from Windows Update
- Block support for partial file download (HTTP range headers)

Windows Update uses dynamically created temporary file names that differ for each computer that downloads updates. This eliminates any benefit that might be gained from caching. Windows Update also uses the Background Intelligent Transfer Service (BITS) as a client, which can request partial files—an operation that the proxy may not support. (Instead, the proxy may support only entire objects.) Larger updates, such as Feature updates, can be tailored by the Windows Update servers to each individual computer.

Resolution

To resolve this issue, make sure that the proxy doesn't try to perform any of the operations that are described in the "Cause" section on Windows Update traffic. For a list of the URLs that are used by Windows Update, see Can't download updates from Windows Update from behind a firewall or proxy server.

If you're using a Bluecoat proxy, you can find more details at Microsoft Windows updates fail to install.

> **Third-party information disclaimer**
>
> Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

Surface Hub may install updates and restart outside maintenance hours

Article • 01/03/2023

Under specific circumstances, Surface Hub installs updates during business hours instead of during the regular maintenance window. The device then restarts if it is necessary. You cannot use the device until the process is completed.

> **Note**
>
> This isn't expected behavior for missing a maintenance window. It occurs only if the device is out-of-date for a long time.

Cause

To ensure that Surface Hub remains available for use during business hours, the Hub is configured to perform administrative functions during a maintenance window that is defined in Settings (see "References," below). During this maintenance period, the Hub automatically installs any available updates through Windows Update or Windows Update for Business (WUfB). Once updates are complete, the Hub may restart.

Updates can be installed during the maintenance window only if the Surface Hub is turned on but not in use or reserved. For example, if the Surface Hub is scheduled for a meeting that lasts 24 hours, any updates that are scheduled to be installed will be deferred until the Hub is available during the next maintenance window. If the Hub continues to be busy and misses multiple maintenance windows, the Hub will eventually begin to install and download updates. This can occur during or outside the maintenance window. Once the download and installation has begun, the device may restart.

To avoid this issue

It's important that you set aside maintenance time for Surface Hub to perform administrative functions. Reserving the Surface Hub for 24 hour intervals or using the device during the maintenance window delays installing updates. We recommend that you not use or reserve the Hub during scheduled maintenance period. A two-hour window should be reserved for updating.

One option that you can use to control the availability of updates is Windows Update for Business.

Learn more

- Maintenance window

Top support solutions for Microsoft Surface Hub

Article • 01/03/2023

Microsoft regularly releases both updates and solutions for Surface Hub. To ensure your devices can receive future updates, including security updates, it's important to keep your Surface Hub devices updated. For a complete listing of the update history, see Surface Hub update history and Known issues and additional information about Microsoft Surface Hub.

> **Tip**
>
> Looking for **Surface Hub warranty information**?

These are the top Microsoft Support solutions for common issues experienced when using Surface Hub.

Setup and install issues

- Setup troubleshooting
- Exchange ActiveSync errors

Miracast issues

- Troubleshoot Miracast on Surface Hub

Download updates issues

- Surface Hub can't download updates from Windows Update

Connect app issues

- The Connect app in Surface Hub exits unexpectedly

Surface Hub 2S adoption and training guides

Article • 01/27/2023

Whether you're a small or large business, a Surface Hub adoption plan is critical in generating the right use cases and helping your users become comfortable with the device. Check out these downloadable guides designed to help you deliver training across your organization.

> **Tip**
>
> As a companion to the adoption kit, we recommend using the **Surface Hub and Microsoft Teams Rooms automated setup guide** when signed in to the Microsoft 365 Admin Center. This guide will customize your experience based on your environment. If you're hosted in Exchange Online and using Microsoft Teams, the guide will automatically create your device account with the correct settings. Or use it to validate existing resource accounts to help turn them into compatible Surface Hub device accounts. To review best practices without signing in and activating automated setup features, go to the **M365 Setup portal**.

On-demand training

- Surface Hub 2S adoption and training videos

Adoption toolkit

- Surface Hub adoption toolkit

Training guides

- Training guide – end user
- Training guide – power user
- Training guide – help desk
- Training guide – Microsoft Teams desktop

Download all training guides

End user guides

- Guide to Navigation on Surface Hub
- Guide to Microsoft 365 on Surface Hub
- Guide to Microsoft Whiteboard on Surface Hub
- Guide to Microsoft Teams on Surface Hub

Download all end user guides

Quick reference cards

- Connect your PC
- Join a Teams Meeting
- Manage a Teams meeting
- Navigation basics
- Schedule a Teams meeting
- Start a new Teams meeting
- Share or send a file
- Sign in to view meetings and files
- Whiteboard advanced
- Whiteboard tools

Download all quick reference cards

Surface Hub adoption welcome screens

- Download or customize adoption welcome screens

Surface Hub 2S on-demand adoption and training videos

Article • 01/26/2023

This page contains comprehensive training for Surface Hub 2S, available on demand.

Chapter 1 - Training overview

https://www.microsoft.com/en-us/videoplayer/embed/RE46Jud?postJsllMsg=true

- Welcome and introduction
- Training overview and agenda
- Software and technology reference
- Surface Hub messaging
- Industries and user roles
- Overview of training services
- Training best practices

Chapter 2 - Getting started with Surface Hub

https://www.microsoft.com/en-us/videoplayer/embed/RE46Ejt?postJsllMsg=true

- What is Surface Hub?
- Technical overview
- Steelcase Roam and the mobility story
- Surface Hub services
- Getting started with Surface Hub
- Gathering expectations

Chapter 3 - Navigating Surface Hub

https://www.microsoft.com/en-us/videoplayer/embed/RE46OFW?postJsllMsg=true

- Welcome screen
- Start menu
- Full screen
- Clip to Whiteboard
- Task bar menu
- Teams/Skype

- End Session

Chapter 4 - Whiteboarding and collaboration

https://www.microsoft.com/en-us/videoplayer/embed/RE46M4v?postJsllMsg=true

- Whiteboard introduction
- Starting the Whiteboard
- Whiteboard tools
- Inserting pictures
- Changing the background
- Sharing the whiteboard
- Export the Whiteboard

Chapter 5 - Exploring Surface Hub apps

https://www.microsoft.com/en-us/videoplayer/embed/RE46Ejz?postJsllMsg=true

- Surface Hub apps introduction
- PowerPoint overview
- Microsoft Word
- Microsoft Excel
- Microsoft Edge

Chapter 6 - Advanced apps and Microsoft 365

https://www.microsoft.com/en-us/videoplayer/embed/RE46EjA?postJsllMsg=true

- Advanced apps introduction
- Microsoft Maps
- Photos
- Power BI
- Sign in to Microsoft 365
- OneDrive
- CoAuthor documents

Chapter 7 - Connecting devices

https://www.microsoft.com/en-us/videoplayer/embed/RE46M4w?postJsllMsg=true

- Connect introduction

- Miracast overview
- Touch and Pen Input
- Wired connect overview
- Line of Business app workflows
- Troubleshooting Miracast and wired connect

Chapter 8 - Skype for Business meetings

https://www.microsoft.com/en-us/videoplayer/embed/RE46M4x?postJsllMsg=true

- Introduction to Skype for Business -Scheduling Skype for Business meetings
- Start a meeting
- Start an ad hoc meeting
- Join a meeting on your calendar
- Managing a Skype for Business meeting
- Present content

Chapter 9 - Microsoft Teams meetings

https://www.microsoft.com/en-us/videoplayer/embed/RE46OFZ?postJsllMsg=true

- Introduction to Microsoft Teams
- Scheduling Microsoft Teams meetings
- Start a meeting
- Start an ad hoc meeting
- Join a meeting on your calendar
- Managing a Microsoft Teams meeting
- Present content
- Conclusion

Chapter 10 - Basic troubleshooting

https://www.microsoft.com/en-us/videoplayer/embed/RE46z65?postJsllMsg=true

- Introduction to Surface Hub troubleshooting
- Application troubleshooting
- End Session
- Restart the device
- Power cycle the device
- Factory reset
- Settings

- Manage Surface Hub
- Conclusion

Surface Hub 2S adoption welcome screens

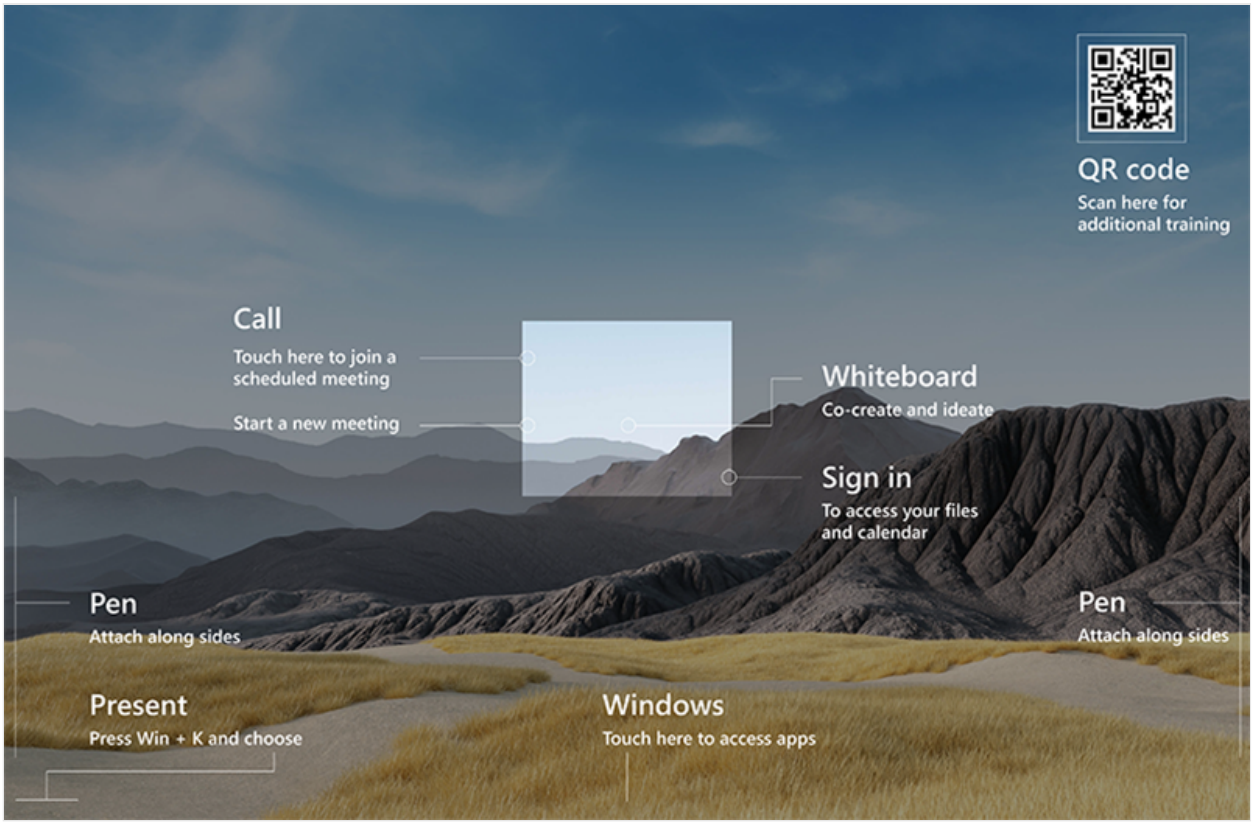
Article • 01/09/2023 • Applies to: Surface Hub 2S

Surface Hub adoption welcome screens are designed to help Surface Hub users get started quickly with call-outs for everyday tasks and a QR code for quick access to adoption resources. This page provides downloadable adoption welcome screens optimized for Surface Hub 2S 50" or Surface Hub 2S 85" devices.

- Download the appropriate file from the following sections and upload the welcome screen to Surface Hub.
- Or customize your own welcome screen using the background of your choice.

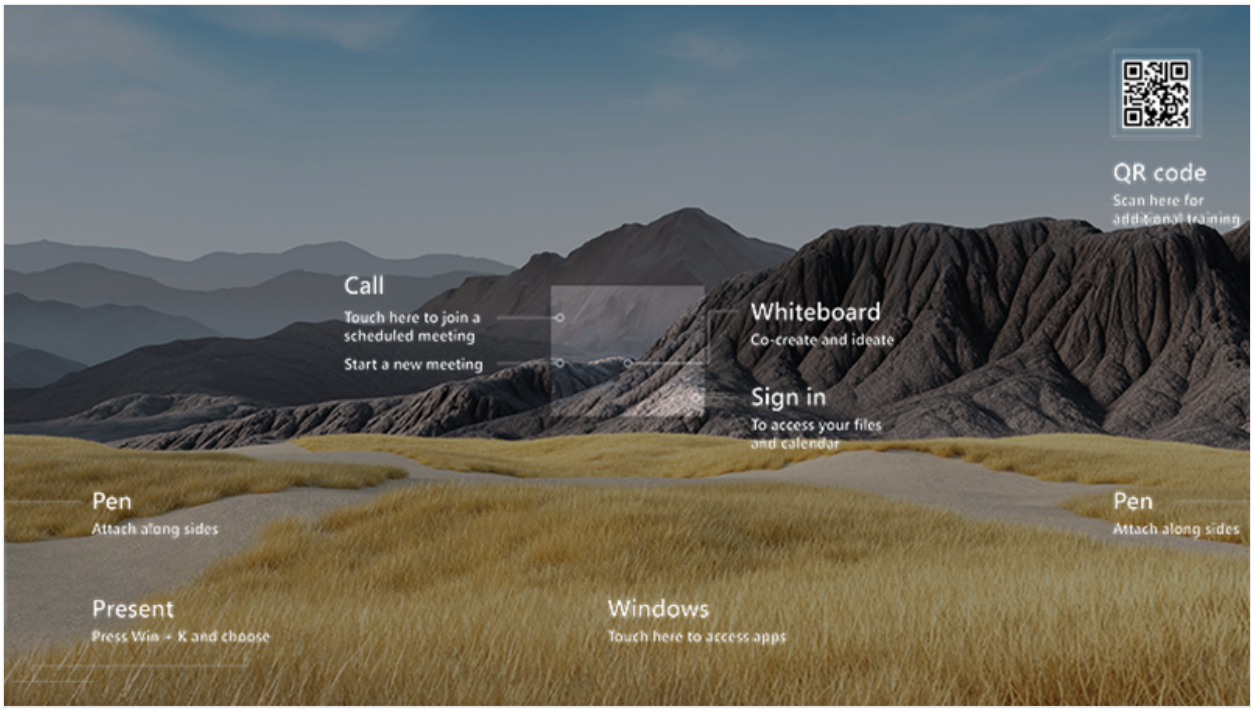
Surface Hub 2S 50” welcome screen

Download optimized welcome screen file for Surface Hub 50"



Surface Hub 2S 85” welcome screen

Download optimized welcome screen file for Surface Hub 85"



Customize welcome screen

To customize your own adoption welcome screen:

1. Browse for the Surface Hub background of your choice. Download the desired background and save it to your local PC.
2. Download the appropriate overlay file:

- Surface Hub 2S 50” overlay
- Surface Hub 2S 85” overlay

3. Open your background image using Adobe Photoshop or a freely available app such as the image editor included in Microsoft PowerToys, downloadable from the Microsoft Store.
4. Open your overlay image. Select and copy the overlay image and paste it onto your background image. Select **Save**.
5. Resize the image to meet or approximate the recommended resolution for your Surface Hub (3840 x 2560 for 50" or 3840 x 2160 for 85").
6. Export the image as a .PNG file and save it to a USB flash drive. (Or save it to a cloud service you can access from Surface Hub).

Upload welcome screen

1. If using a USB flash drive, plug it into an available port on Surface Hub.
2. Sign in to Surface Hub 2S with an Admin account.
3. Open **Settings** > **Welcome Screen**.

4. Under **Background for welcome screen**, choose **Photo 2** and **Browse** to locate your welcome screen image from your USB flash drive or cloud service.
5. Your new welcome screen appears under **Preview**.

Surface Hub return to the office video series

Article • 01/03/2023

This page features instructional videos to help keep your Surface Hub devices up to date and functioning as expected when returning to the office. Learn about new features of the Surface Hub operating system and updated applications and enhancements to the overall Surface Hub experience.

Video	Description	Learn more
How to verify a Surface Hub is fully updated	Discover the build number a Surface Hub is currently running and determine if it's fully updated. Learn why a Surface Hub may not be installing updates.	Surface Hub update history
How to verify Device Account and User Sign-In are working on a Surface Hub	Learn how to verify the device account and user sign-in experience.	Create and test a device account
How to use Teams Rooms on Surface Hub client	See the latest features for Teams Rooms and how to use Coordinated Meetings and Proximity Join.	Microsoft Teams Rooms on Surface Hub
How to use Modern Authentication on Surface Hub	Learn the requirements for using Modern Authentication for the device account as well as disabling the feature in unsupported environments.	Modern authentication on Surface Hub

Learn more

- Known issues: Windows 10 Team

Surface Hub 2S 50-inch tech specs

Article • 01/03/2023

Item	Details
Dimensions	29.2" x 43.2" x 3.0” (741 mm x 1097 mm x 76 mm)
Shipping dimensions	47.64" x 36.89" x 9.92" (1,210 mm x 937 mm x 252 mm)
Weight	61.6 lbs. (28 kg)
Shipping Weight	81.08 lbs. (36.77 kg)
Display	PixelSense Display, 3:2 aspect ratio, 10-bit color, 15.5 mm border, anti-glare, IPS LCD
Resolution	3840 x 2560 (4K UHD)
Contrast	1200:1 (typical), 1000:1 minimum
Brightness	350 nits (typical)
Processor	Quad-core 8th Generation Intel Core i5 processor, 8 GB RAM, 128 GB SSD[1]
Graphics	Intel UHD Graphics 620
Wireless	Wi-Fi 5 (IEEE 802.11 a/b/g/n/ac compatible) Bluetooth Wireless 4.1 technology Miracast display
Connections	USB-A Mini-DisplayPort 1.2 video output RJ45 gigabit Ethernet (1000/100/10 BaseT) HDMI video input (HDMI 2.0, HDCP 2.2 /1.4) USB-C with DisplayPort input Four USB-C (on display)
Sensors	Doppler occupancy[2] Accelerometer Gyroscope
Audio/Video	Full-range, front facing 3-way stereo speakers Full band 8-element MEMS microphone array certified for use with Microsoft Teams up to 2.3 meters away Microsoft Surface Hub 2 Camera, 4K, USB-C connection, 90-degree HFOV
Pen	Microsoft Surface Hub 2 Pen (active)

Item	Details
Software[3]	Windows 10 Microsoft Teams for Surface Hub Skype for Business Microsoft Whiteboard Microsoft Office (Mobile) Microsoft Power BI
Exterior	Casing: Precision machined aluminum with mineral-composite resin Color: Platinum Physical Buttons: Power, Volume, Source
What's in the box	One Surface Hub 2S One Surface Hub 2 Pen One Surface Hub 2 Camera 2.5 m AC Power Cable Quick Start Guide
Warranty	1-year limited hardware warranty[4]
BTU	1518 BTU/hr
Input Voltage	50/60Hz 110/230v nominal, 90-265v max
Input power, operating	445 W (495 W Surge Load)
Input Current	5.46 A
Input Power, standby	5 W max

Note

[1] System software uses significant storage space. Available storage is subject to change based on system software updates and apps usage. 1 GB= 1 billion bytes. See Surface.com/Storage for more details.
[2] Doppler sensor not available in Hong Kong, India, Kuwait, and Oman due to local regulations.
[3] Software license required for some features. Sold separately.
[4] Microsoft's Limited Warranty is in addition to your consumer law rights.

Note

Surface Hub can be used continuously for a maximum of 18 hours a day. To optimize for efficiency, Surface Hub uses smart sensors to turn off the LED screen when presence is no longer detected, which means there is no need to power it down at the end of the day. If the unit is installed in a 24-hour workplace environment, the sensors can be disabled to comply with the 18 hour per day maximum use recommendation. Note that prolonged display of a video signal may cause burned-in or image retention to occur on the screen. To learn more about managing power settings, see:

- **Local management Surface Hub settings**
- **SurfaceHub CSP - Windows Client Management**

Surface Hub 2S 85" overview & tech specs

Article • 01/03/2023

The 85" version of the Surface Hub family brings the Surface Hub 2S experience to spaces requiring a larger screen such as conference rooms, board rooms, or larger huddle spaces. Surface Hub 2S 85” delivers the following experiences:

- **Designed for group collaboration.** Invites simultaneous inking in Microsoft Whiteboard plus larger-than-life remote attendees in Microsoft Teams.
- **Consistent Surface Hub 2S experience.** Provides the same premium design, 4K display technology, touch, pen/ink, compute cartridge, and camera support as Surface Hub 2S 50”.
- **Integration with existing and new A/V systems.** Combines with Microsoft Teams certified peripherals and integrates with Microsoft Teams Rooms.

Surface Hub 2S 85" tech specs

Component	Description
Dimensions	44.5” x 77.1” x 3.4” (1130 mm x 1959 mm x 85.6 mm)
Shipping dimensions	89.5” x 62” x 22.8” (2275 mm x 1573 mm x 580 mm)

Component	Description
Weight	185 lbs (84 kg)
Shipping weight	399 lbs (181 kg)
Display	PixelSense™ Display, 16:9 aspect ratio, 10-bit color, 30.5mm border width, anti-glare, IPS LCD, in-cell touch with 20 simultaneous touch points
Resolution	3840 x 2160 (4K UHD)
Contrast ratio	1000:1 (typical), 800:1 (minimum)
Brightness	280 nits (typical)
Compute	Modular Compute Cartridge Quad-core 8th Generation Intel® Core™ i5 processor, 8GB RAM, 128GB SSD[1]
Software[2]	Windows 10 Team OS Microsoft Teams for Surface Hub Skype for Business Microsoft Whiteboard Microsoft Office (Mobile) Microsoft Power BI
Connections	USB-A Mini-DisplayPort Video Output RJ45 Gigabit Ethernet HDMI Video Input USB-C® with DisplayPort Input (3) USB-C® (on display)
Graphics	Intel® UHD Graphics 620
Audio/video	100Hz - 12KHz range 3-way stereo speakers, including (2) mid/high-range and (1) mid/low-range in rear bump. Full band 8-element MEMS microphone array certified for use with Microsoft Teams up to 3.5 meters away Microsoft Surface Hub 2 Camera, 4K, USB-C® connection, 90-degree HFOV
Pen	Microsoft Surface Hub 2 Pen (active) Surface Slim Pen compatible
Sensors	Doppler occupancy sensor[3]
Wireless	Wi-Fi 5: IEEE 802.11 a/b/g/n/ac compatible Bluetooth® Wireless 5.0 technology Miracast Display

Component	Description
Exterior	Casing: Precision machined aluminum with mineral-composite resin Color: Platinum Physical Buttons: Power, Volume, Source
What's in the box	(1) Surface Hub 2S (2) Surface Hub 2 Pen (1) Surface Hub 2 Camera 4m AC Power Cable Quick Start Guide
Warranty	1-year limited hardware warranty[4]
BTU	2047 BTU/hr
Input Voltage	50/60Hz 110/230v nominal, 90-265v max
Input power, operating	665 W (745 W Surge Load)
Input Current	7.8 A
Input Power, standby	5 W max

> ⓘ **Note**
>
> Surface Hub can be used continuously for a maximum of 18 hours a day. To optimize for efficiency, Surface Hub uses smart sensors to turn off the LED screen when presence is no longer detected, which means there is no need to power it down at the end of the day. If the unit is installed in a 24-hour workplace environment, the sensors can be disabled to comply with the 18 hour per day maximum use recommendation. Note that prolonged display of a video signal may cause burned-in or image retention to occur on the screen. To learn more about managing power settings, see:
>
> - **Local management Surface Hub settings**
> - **SurfaceHub CSP - Windows Client Management**

References

1. System software and updates use significant storage space. Available storage is subject to change based on system software and updates and apps usage. 1 GB = 1 billion bytes. 1 TB = 1,000 GB. See Surface Storage for more details.
2. Software license required for some features. Sold separately.
3. Doppler sensor not available in Hong Kong, India, Kuwait, and Oman.
4. Microsoft's Limited Warranty is in addition to your consumer law rights.

Learn more

- Surface Hub 2S 85" - Collaboration at a Massive Scale

Surface Hub 2S site readiness guide

Article • 01/03/2023

Topic	Description
Site planning for Surface Hub 2S	Review room considerations and planning for peripherals.
Surface Hub 2S quick start	Get an overview of required steps to unpack and start Surface Hub 2S.
Install and mount Surface Hub 2S	Learn about licensed accessories to install and mount Surface Hub 2S.
Moving and handling Surface Hub 2S 85"	Learn about safe safely moving Surface Hub 2S 85" into a commercial space.
Install and mount Surface Hub 2S 85"	Review recommended guidance for installing Surface Hub 2S 85".
Customizing installation of Surface Hub 2S	Learn how to custom install without licensed mounting accessories.
Surface Hub 2S ports and keypad overview	Get details for I/O ports and keypad power and selection controls.
Connect to Surface Hub 2S	Learn about wired and wireless methods to connect to Surface Hub.

Surface Hub 2S site planning

Article • 01/03/2023

Designed for team collaboration, Surface Hub 2S can transform the way you work — not only in the conference rooms but any place you want to work. One of the biggest advantages of Surface Hub 2S is the ability to move it from one space to another when used with the Steelcase Roam mobile stand and mobile battery. Providing unplugged, uninterrupted teamwork capabilities, Surface Hub 2S can be integrated into almost any workspace.

Room considerations

Designed for interactive use in smaller conference rooms and huddle spaces, Surface Hub 2S provides a 4K camera, microphone array, crystal clear speakers, and a brilliant 4K+ resolution display. Optimizing the user experience in larger spaces with more people further away from the display may require peripherals such as an extra camera, microphone, or room systems solution such as Microsoft Teams Rooms.

As a general guideline, install Surface Hub 2S in a space that meets the following criteria:

- People can reach all four edges of the touchscreen.
- The screen is not in direct sunlight, which could affect viewing or damage the screen.
- Ventilation openings are not blocked.
- Microphones are not affected by noise sources, such as fans or vents.
- Space is well lit with no reflective sources.

Whether mounted to a wall or installed on the mobile stand, the areas where you use the device should maintain:

- Room temperatures no cooler than 10°C (50° F) and no hotter than 35°C (95° F).
- Relative humidity no lower than 20 percent and no higher than 80 percent.

For detailed room planning guidance and more information about Microsoft Teams Rooms see Plan Microsoft Teams Rooms.

Managing Surface Hub 2S location

If you plan to use Surface Hub 2S on a mobile stand, you may wish to explore third-party solutions that enable location services. For example, active RFID systems can

provide real-time tracking throughout complex office or industrial spaces. For more information, see your A/V provider or other third-party expertise for guidance.

Surface Hub 2S quick start

Article • 01/03/2023

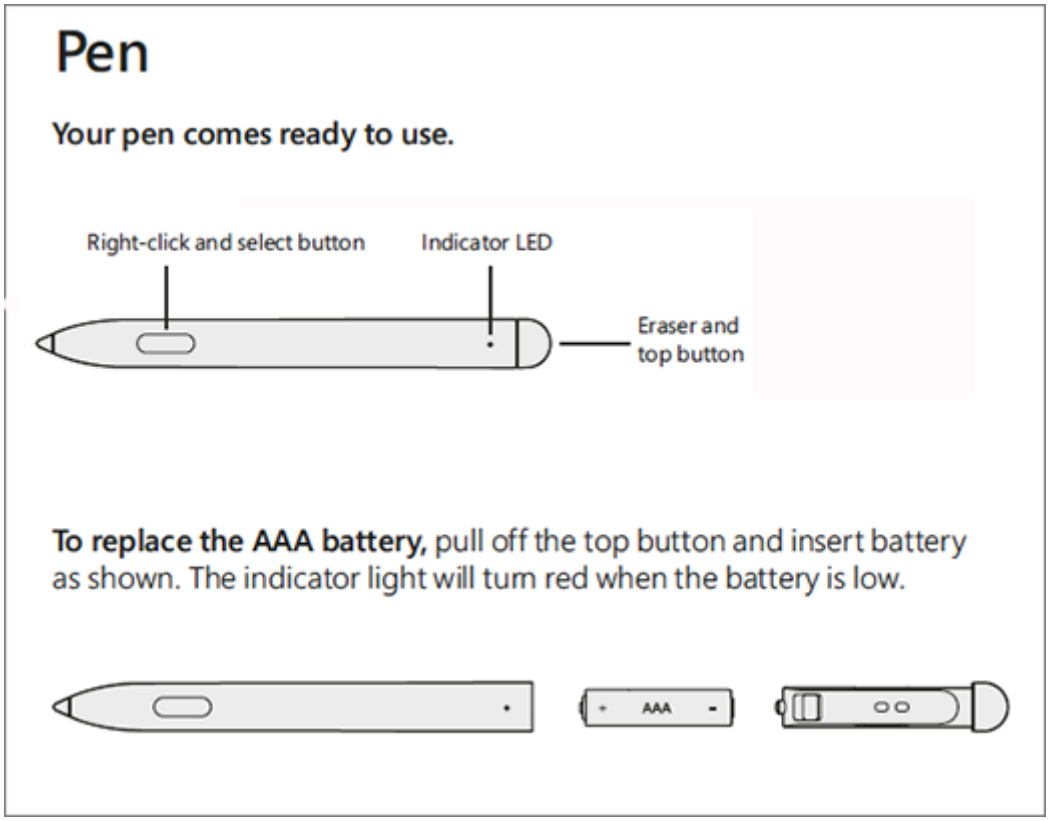
Unpack Surface Hub 2S

1. Use the handles on each side of the box to move it to the space where you'll set it up.
2. Before opening, remove the clips (4) on the front and back, and then lift the top off the box using the handles.
3. In the base of the Surface Hub 2S, open the accessories box containing the setup guide, Surface Hub 2 pen, Surface Hub 2 camera, and the power cable.
4. On the back of the Surface Hub, there's an instructional label showing you where to attach the mounting hardware. Install them in place and remove the label.

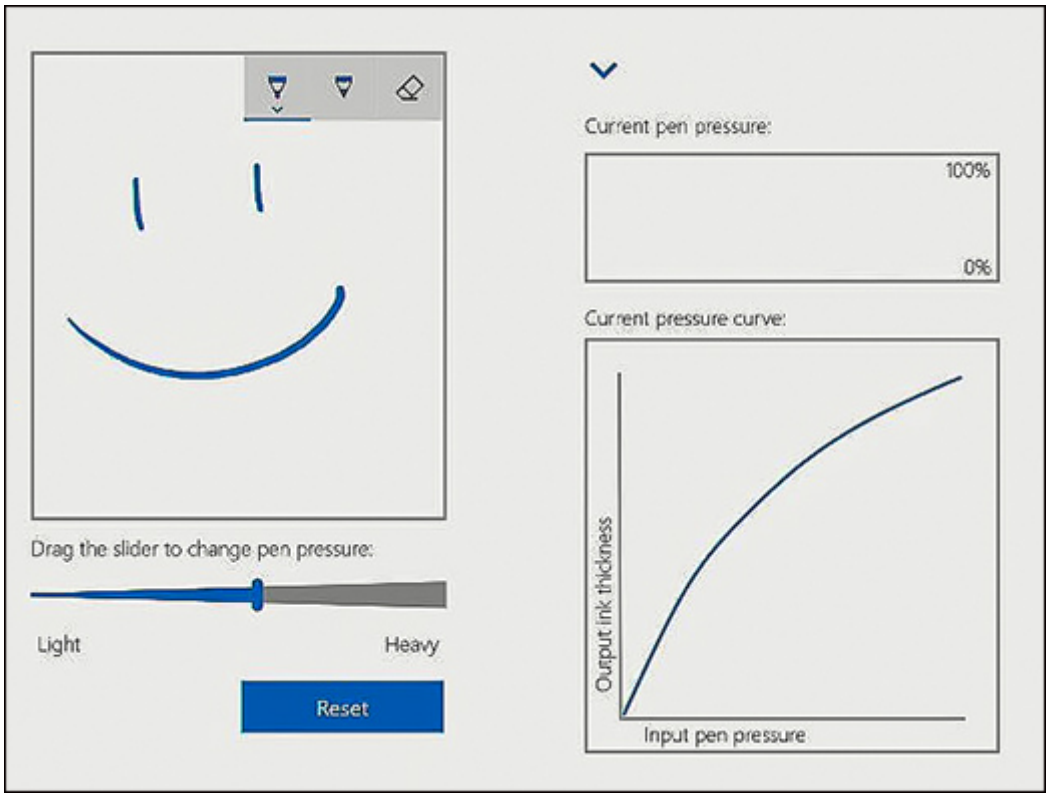
See this video for more information about unboxing and set up.

Install and adjust pen

1. Attach Surface Hub 2 pen magnetically to your preferred side of the device.



2. To adjust pen pressure, open the Surface app on Surface Hub 2S, select Pen, and adjust the slider.



Install camera

Remove the lens cling from the camera and attach it to the USB-C port on the top of the Surface Hub 2S.

Start Surface Hub 2S

1. Insert the power cable into the back of the device and plug it into a power outlet. Run the cable through any cable guides on your mounting solution and remove the screen clang.
2. To begin, press the power button on the bottom right.

Unpack Surface Hub 2S

Article • 01/03/2023

Unpacking Surface Hub 2S

Before you remove Surface Hub 2S from the box, make sure that you have your mounting solution assembled and someone available to help you.

1. Use the handles on each side of the box to move it to the space where you'll set it up.
2. Before opening, remove the clips (4) on the front and back, and then lift the top off the box using the handles.
3. In the base of the Surface Hub 2S, open the accessories box containing the setup guide, Surface Hub 2 pen, Surface Hub 2 camera, and the power cable.
4. On the back of the surface hub, there's an instructional label that shows you where to attach the mounting hardware. Install them in place and remove the label.
5. If you're using a mobile stand remember to lock the wheels to keep the stand in place
6. Be sure to lift the Surface Hub 2S with both hands and support the bottom of the device.
7. Align the installed hardware with the slots on the mount so it rests firmly in place.
8. Follow any further instructions that came with your mounting solution.

Install pen and camera

1. Unwrap your Surface Hub 2 pen and attach it magnetically to your preferred side of the device.
2. Remove the lens cling from the camera and attach it to the USB-C port on the top of the Surface Hub 2S.
3. Insert the power cable into the back of the device and plug it into a power outlet. Run the cable through any cable guides on your mounting solution and remove the screen clang.
4. To begin, press the power button on the bottom right.

Install and mount Surface Hub 2S 50"

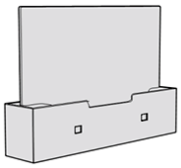
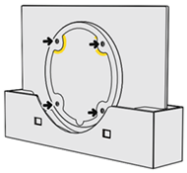
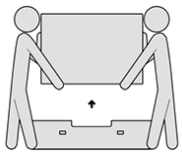
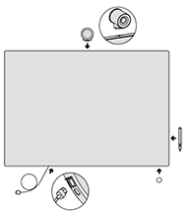
Article • 04/19/2023

Surface Hub 2S 50" is designed for ease of mobility with a form factor that enables you to quickly install and begin using the device. Microsoft has partnered with Steelcase on the following certified mounting solutions: Roam Mobile Stand and Roam Wall Mount. Both fully integrate with the design of Surface Hub 2S 50", enabling unimpeded access to the compute cartridge, power, USB-A, USB-C, and other ports.

You can mount Surface Hub 2S 50" with the certified wall mount or the certified mobile stand, both developed in partnership with Steelcase. Both fully integrate with the design of Surface Hub 2S 50", enabling unimpeded access to the compute cartridge along with all I/O ports and power.

For more information, see Officially licensed third-party accessories and view installation demos from the Surface product team at Steelcase mobile stand and APC battery set up.

If you're not using licensed accessories, see Customize wall mount of Surface Hub 2S 50".

Task	Illustration
1. Set up your mount first	
Leave your Surface Hub in the box until the mount is set up and mounting hardware is applied. Mount isn't included. Your mount is sold separately.	
2. Attach hardware to the Surface Hub	
Mounting hardware and specific instructions are found in the box for your mount.	
3. Remove the instructional label before mounting.	
Get someone to help you lift and mount your Surface Hub. Make sure to hold and lift the Surface Hub from the bottom.	
4. Attach accessories and power on	
Install accessories and attach power cable as shown. See guides on the screen cling. Remove cling wrap from the screen. Press the power button to power on.	

Install and mount Surface Hub 2S 85”

Article • 01/03/2023

This article explains how to physically install Microsoft Surface Hub 2S 85" in commercial environments.

Unboxing video

Before you begin, please review Microsoft Surface Hub 2S 85" Unboxing and Set Up video:
https://www.microsoft.com/en-us/videoplayer/embed/RWwwgL?postJsllMsg=true

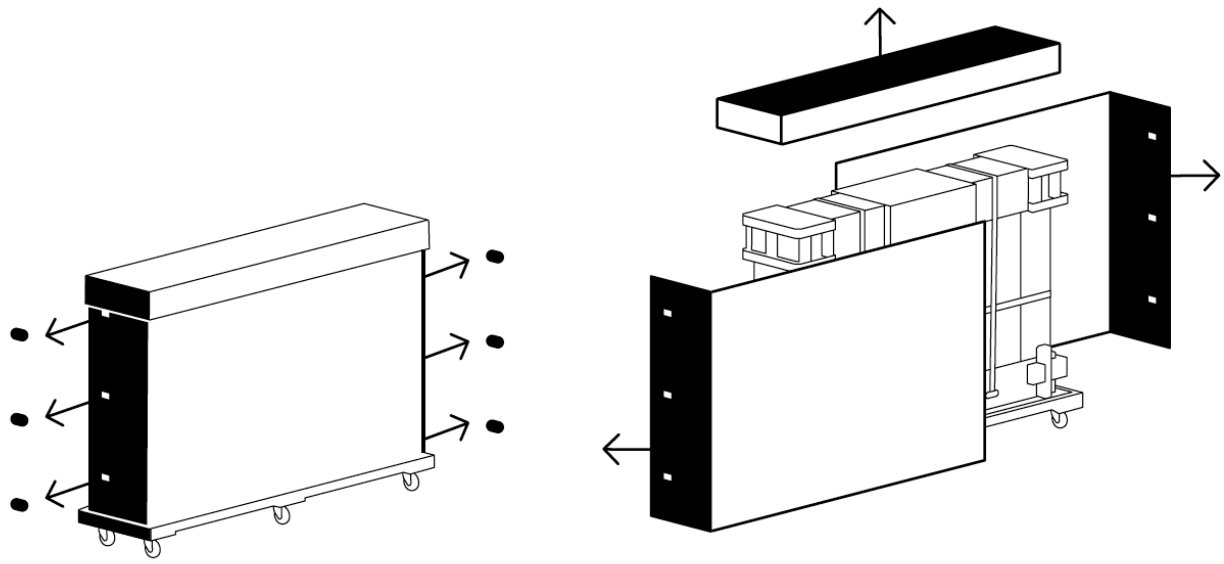
Follow all safety precautions

> ⚠ **Warning**
>
> **Handling and site prep**
>
> - The device is very heavy. To reduce the risk of personal injury, death, or damage to the device due to its size and weight, it is important to keep the device upright.
> - Before moving the device to the place where it will be installed, survey the site to determine how to safely move it to the location where it will be unpacked and mounted.
> - Always use at least two people for unpacking and installation.
> - Once the device is unpacked, it should be mounted immediately, so the mounting system should be in place before unpacking. If you’re mounting onto a rolling stand, lock or block the wheels of the stand before unpacking.
> - To avoid tripping hazards, keep the assembly area clear of packing materials.

> ⓘ **Important**
>
> Before proceeding, review the additional safety information listed in **Appendix A** below.

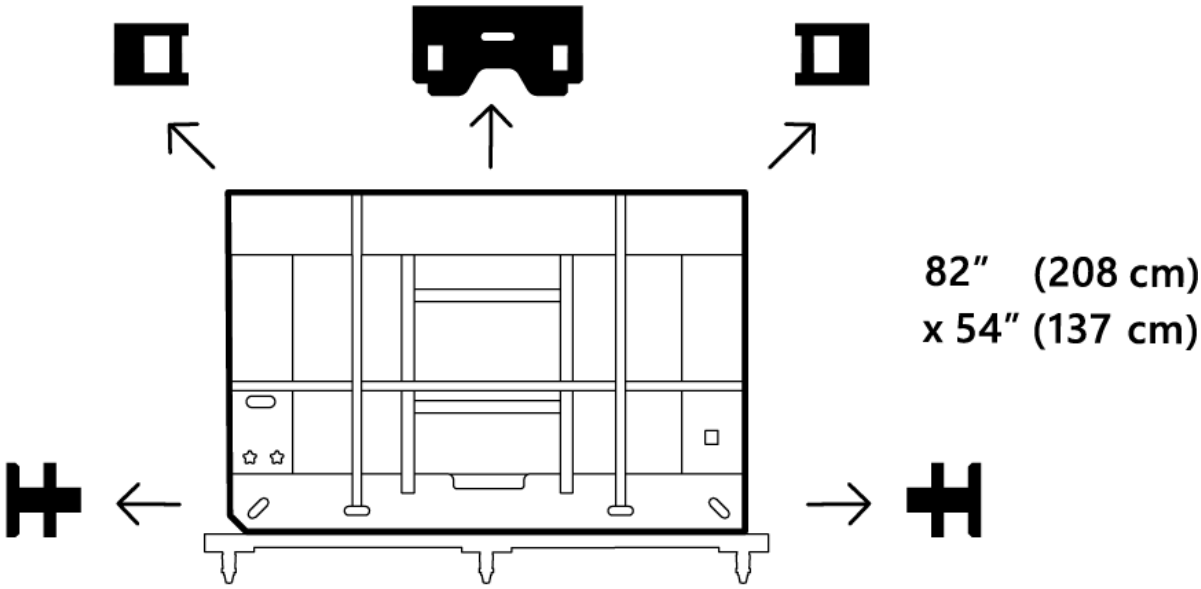
1. Remove outer packaging materials

1. Remove and recycle outer cover.
2. Cut four (4) plastic straps.
3. Open and remove the six (6) clips from the ends.
4. Remove lid and then lift and remove front and back panels.



2. Remove black outer packaging foam

1. Remove black corner foam pieces (4).
2. Remove black center foam support.



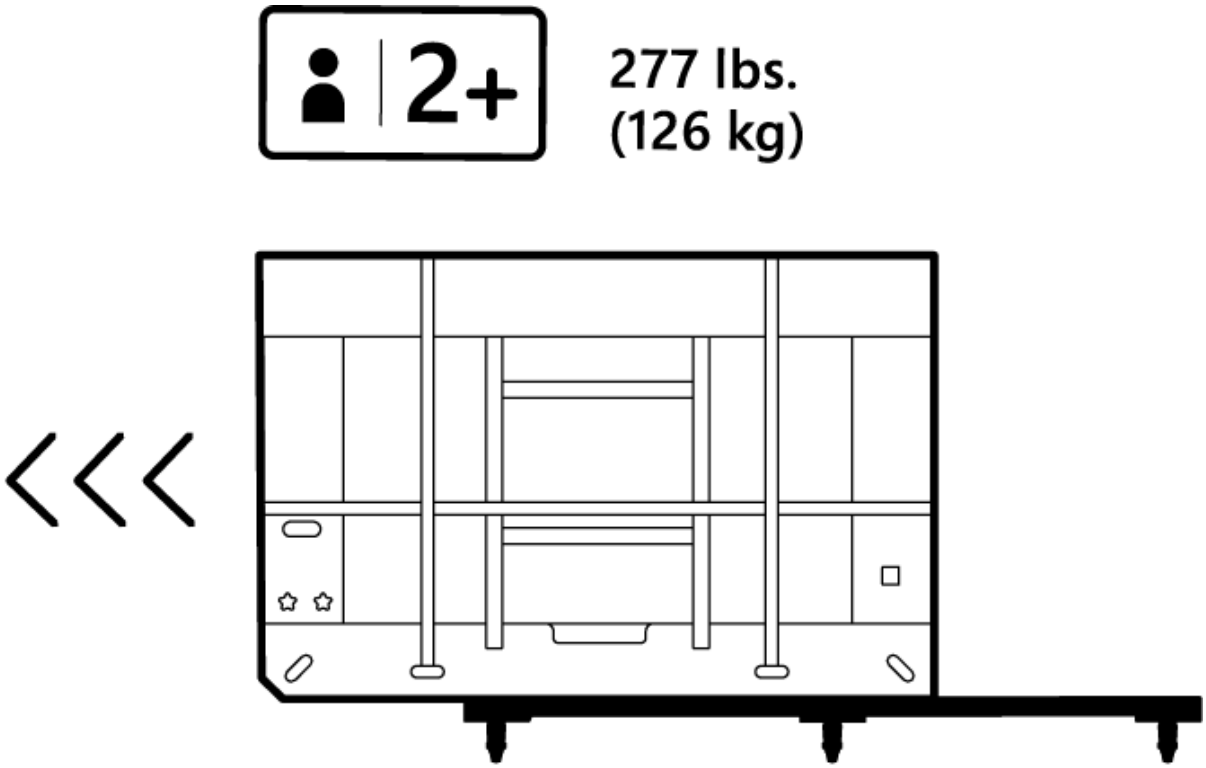
⊗ Caution

Do not remove any white foam, strapping or packaging materials until the Hub 2S is adjacent to the cart or wall mount on which it will be placed. Additional strapping materials are provided in the small box located under the hand screw knobs on the

back side of the package. Original or replacement strapping materials must be in place before moving and especially before rotating the device and its protective package

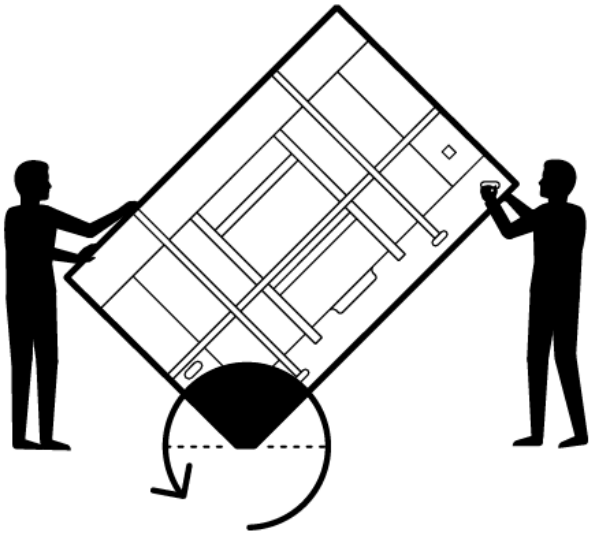
3. Remove inner packaging frame from pallet

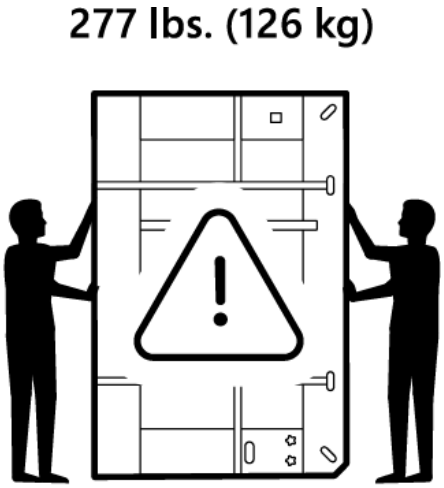
1. Move pallet assembly to elevator location.
2. Lock wheel brakes (4).
3. Slide inner packaging off pallet.



4. Rotate packaging frame to fit elevator

1. Rotate frame to fit elevator
2. Rotate on beveled end of inner frame and slide into the elevator.



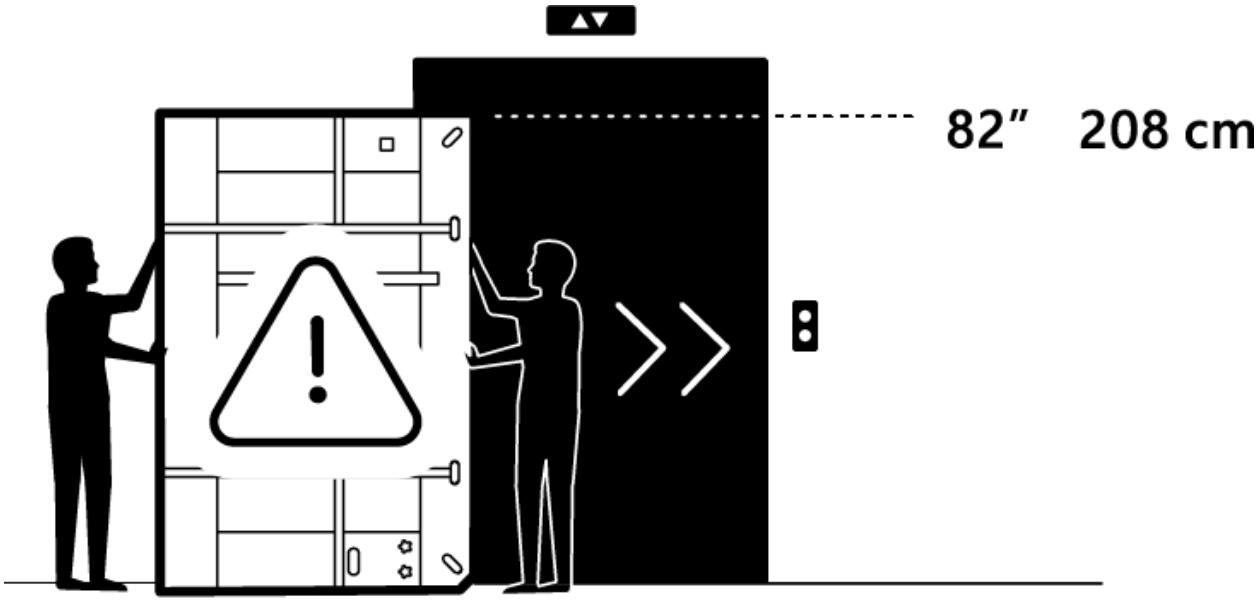


Tip

The wheeled pallet is custom fit to the inner frame packaging footprint and can be used throughout the installation site delivery process. Inner wood frame end piece has nylon skid plates.

5. Remove from elevator

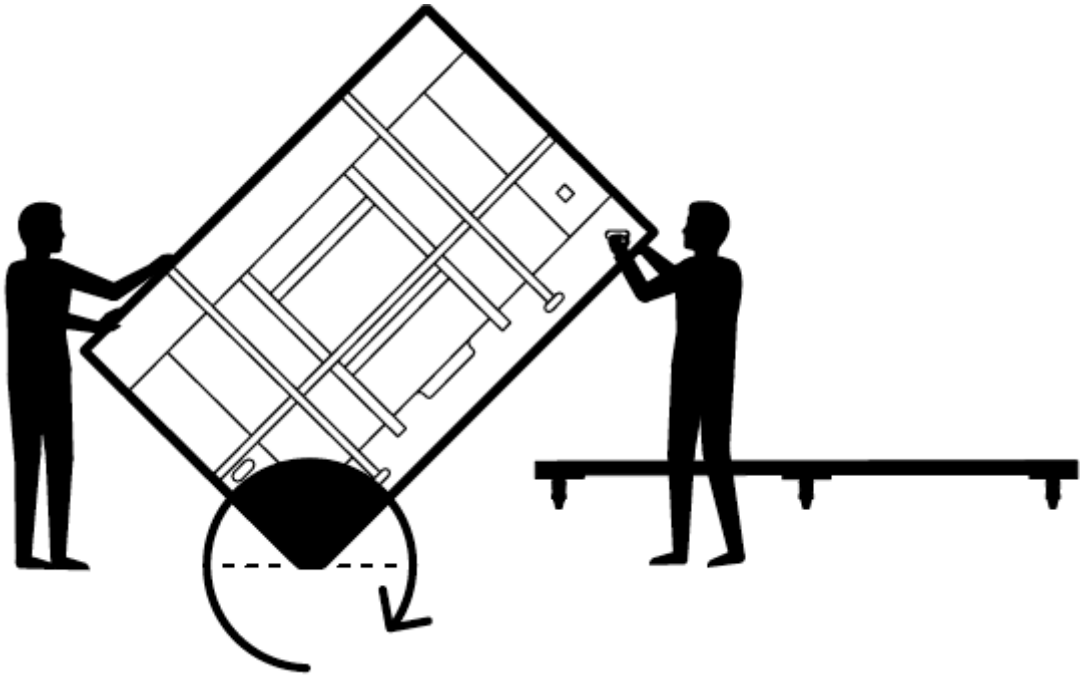
1. Slide out of elevator
2. Lock wheel brakes (x4).



6. Place Surface Hub 85” back on pallet

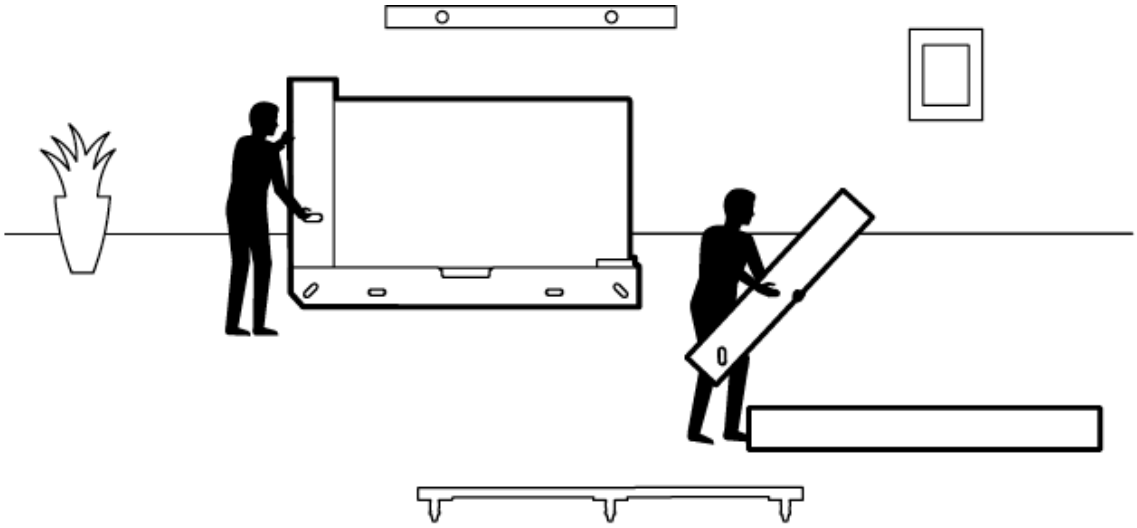
1. Using beveled end, rotate back onto pallet.

2. Unlock wheel brakes (x4).
3. Move product to location of wall or cart mount.



7. Place Surface Hub 85" on Wall Mount or Cart

1. Place Hub 2S in front of wall mount or cart.
2. Lock wheel brakes (x4).
3. Slide inner packaging off pallet.
4. Cut the 3 plastic straps.
5. Remove lid.
6. Remove white foam pieces.
7. Remove Welcome Kit.
8. Remove end piece by lifting vertically.
9. Remove wood end pieces by the four hand knobs screws on the wood base.



> **⊗ Caution**
>
> Do not leave Hub 2S 85" unattended. An additional person is needed to hold device upright. Once end pieces are removed, a minimum of one person needs to maintain contact with the Hub 2S until placement on wall mount or cart is completed.

10. Lift plywood end piece up and back.
11. Remove bump label from back.
12. Lift the Hub 2S from the lower tray and place on cart or wall mount.

> **ⓘ Note**
>
> Following the cart or wall mount manufactures instructions, prepare the mounting system prior to removing the Hub 2S from its inner packaging tray.

> **Tip**
>
> When grasping the Hub 2S, note the hand hold cut outs in the lower foam. Care must be taken care with the top hand not to grasp the device where the speakers are located. Graphic on the ends of the device cover provide general speaker location.

13. Loosen elastic tension clips (x2).
14. Remove cloth cover.

15. Note locations for placement of pens (x2), camera, and power cord.

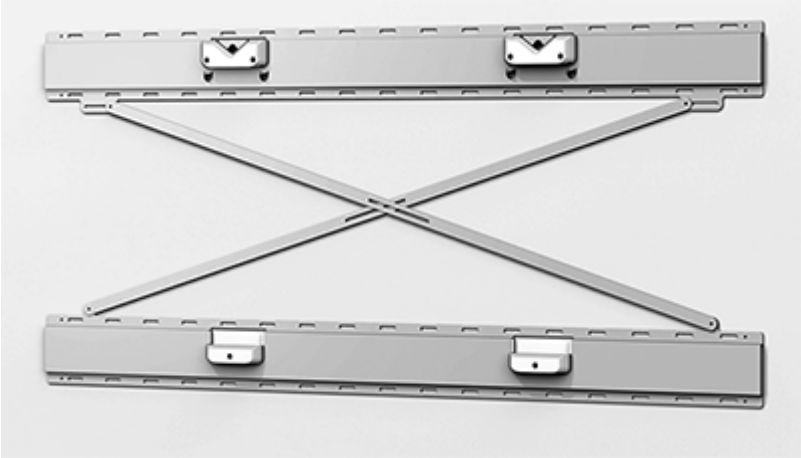
16. Attach pens (x2), camera, and power cord.

17. Remove cling labels (x4).

18. Press the power button on lower right. Installation is now complete.

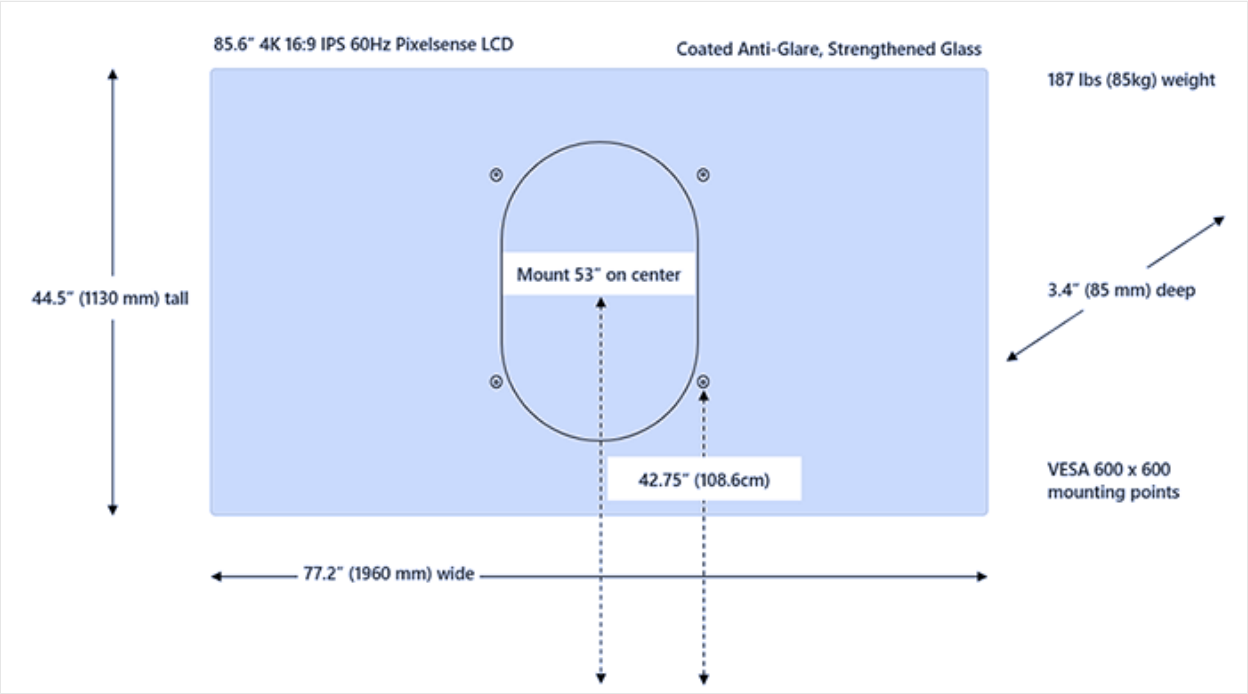
Mounting Surface Hub 2S 85"

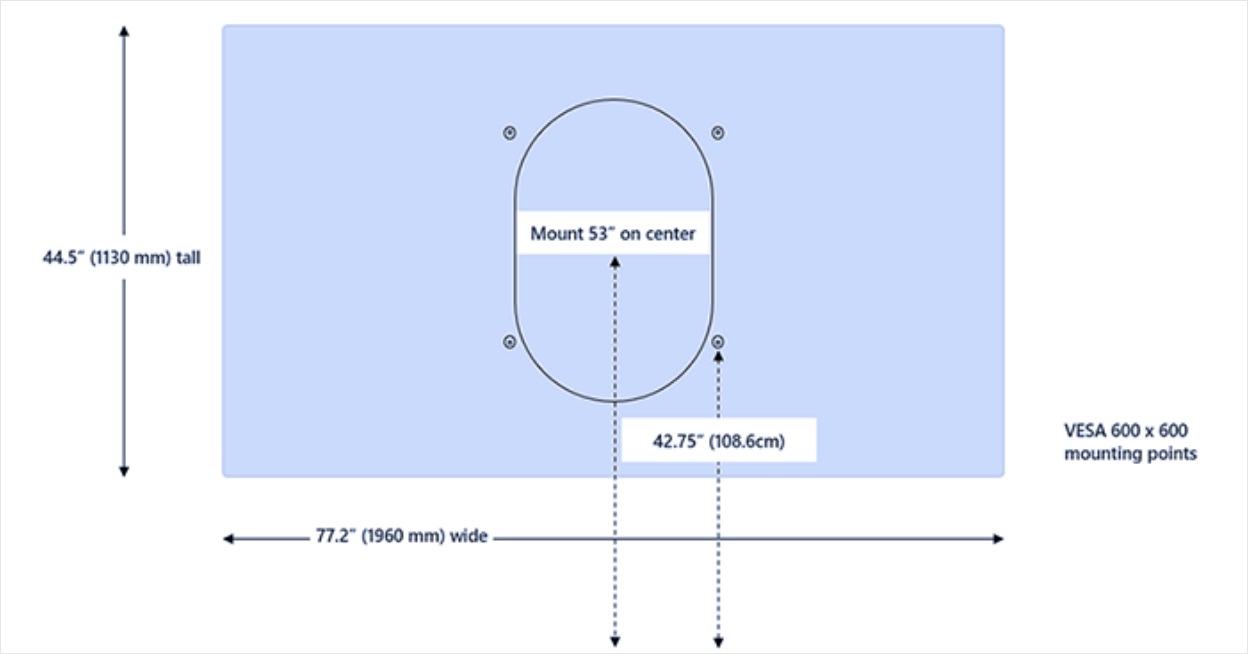
The Surface Hub 2S 85” uses a 600 x 600 VESA mount pattern. As shown in the following image, Microsoft has partnered with Steelcase to create mounting options compatible with the Surface Hub 2S 85” unique design.



Mounting dimensions

If using other (non-Steelcase) mounting options, you will need spacers to account for the compute enclosure on the back of the device. Spacers and other certified accessories are available from Salamander Designs.





Supplemental Strapping Kit

An additional set of inner packaging strapping materials can be found in the kit attached at the back, lower right.

Appendix A: Additional safety information

> ⚠ **Warning**
>
> **Heavy object/ergonomic lifting**
> The device is very heavy. To reduce the risk of lifting-related injuries, death, or

damage to the device, we recommend that a minimum of two or more people lift the device. It is important to use proper lifting posture when lifting and/or moving the device. Use good ergonomic lifting practices, including but not limited to:

- Plan ahead. Make sure the lifting team agrees on the plan.
- Determine if you can lift the unit. Is it too heavy or too awkward?
- Decide if you need lifting aid.
- Check your environment for obstructions and slippery surfaces.
- Lift with your legs, not your back.
- Bend at your knees, keeping the back straight.
- Keep the unit close to your body.
- Center your body over the unit. Keep the feet about shoulder width apart.
- Lift straight up smoothly.
- Keep your torso straight; do not twist while lifting or after the load is lifted

⚠ **Warning**

Proper mounting
The device is heavy and attaches to a cart or wall mount. To reduce the risk of injury, death, or damage to the device:

- Follow all instructions provided by the cart or wall mount manufacturer.
- Ensure the proposed mounting system will support the weight of this device.
- Only use the mounting hardware provided with mounting the system.
- Ensure all screws are securely tightened according to the manufacturer's instructions.
- Do not release the device until you are certain device is fully engaged with mounting system attachment points.
- Microsoft recommends using carts or wall mounting systems designed for use with your device. Microsoft is not responsible for any damage, injuries, or death caused by the use of other mounting systems.

⚠ **Warning**

Unseen hazards in walls or other mounting surfaces
Walls and other mounting surfaces may contain electrical wires, gas lines, and other unseen hazards or obstacles. Cutting or drilling into an unseen hazard may cause serious personal injury or death. It is the installer's responsibility to locate unseen

hazards prior to and to avoid these hazards during installation. Assess the mounting environment and always make sure there are no unseen hazards in the wall or other mounting surface prior to drilling and/or cutting.

⚠ Warning

Tip hazard
To avoid risk of personal injury, death, or damage to a cart/stand-mounted device when it is moved:

- Only use a cart/stand that is compatible with this device.
- Follow all instructions provided by the cart/stand manufacturer for moving or relocating a stand-mounted device.
- Do not hang or place heavy objects from the device or on the cart/stand.
- Disconnect the power cord and other cables as needed prior to moving the cart/stand-mounted device. Use caution and move slowly when moving cart/stand-mounted device. Follow the cart/stand manufacturer's instructions for moving or relocating the stand.
- Use caution when transporting a cart/stand-mounted device up or down ramps. Never leave a cart/stand-mounted device unattended on or near a ramp.
- Only adults should move the cart/stand-mounted device.

⊗ Caution

Touch-screen glass
The touch screen on the device, like most touch screens, is made of glass. The glass can break if the device is dropped or receives a significant impact. To reduce the risk of personal injury, avoid touching the screen if the glass is broken, chipped or cracked and arrange to have the screen replaced. A cracked or chipped touch screen caused by misuse or abuse of your device is not covered under the product's limited warranty.

⚠ Warning

Proper installation
To avoid hazards related to improper device installation, installation must be performed by people who have read and understand the installation instruction

prior to beginning work. If you do not have the necessary equipment or expertise, or if you are uncertain the mounting surface can properly support consult a professional installer.

More information

- Steelcase Roam Collection
- Salamander Designs

Customize wall mount of Surface Hub 2S 50"

Article • 01/03/2023

This article provides guidance for physically installing the Microsoft Surface Hub 2S 50." For information about installing the 85" see Install and mount Surface Hub 2S 85".

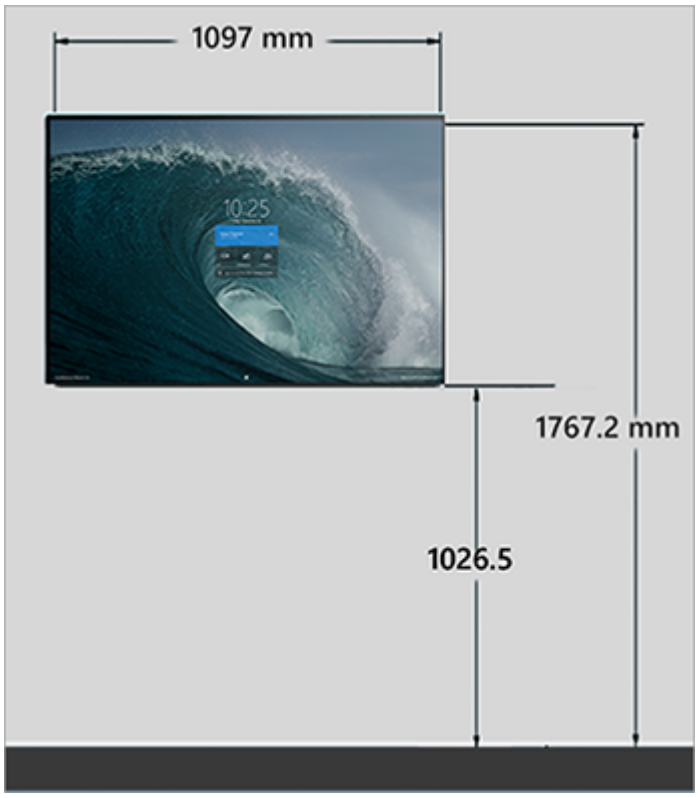
If not using certified mounting solutions, you can mount Surface Hub 2S 50" using readily available retail hardware.

Set wall mount measurements

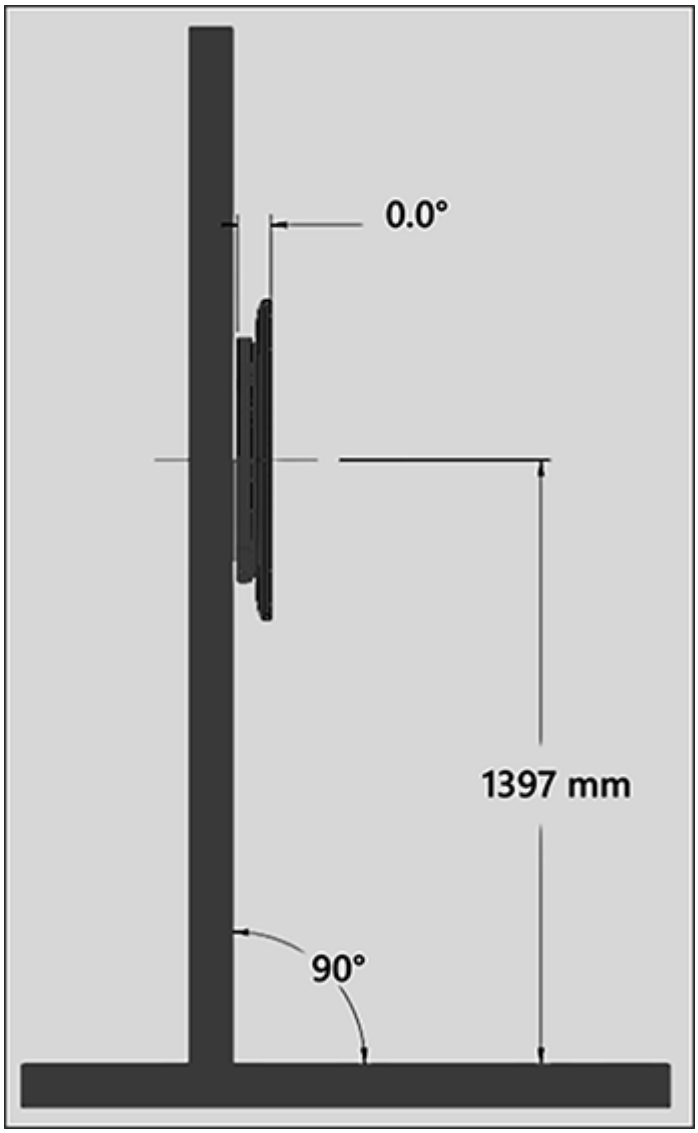
Surface Hub 2S 50" recommended mounting measurements:

Item	Description	Notes
Height from bottom of Surface Hub 2S 50"	1026.5 mm (40.41”)	Recommended
Height from top of Surface Hub 2S 50"	1767.2 mm (69.57”)	Recommended
Height from center of mount	1397 mm (55”)	Recommended

1. Measure 1026.5 mm (40.41”) from the floor level to set the recommended minimum height.
2. Measure 1767.2 mm (69.57”) from the floor level to set the recommended top height.



3. Measure 1397 mm (55”) mm from the floor level to set the recommended center height.



Obstruction free mounting

In addition to the visible ports on the sides of the device, certain integrated components must remain free of obstruction in order to function correctly. These include the Bluetooth, Wi-Fi, occupancy, and mic sensors as well thermal cooling vents. Keep out zones

Item	Description	Notes
Access	Ensure unimpeded access to input/output ports, the compute cartridge, Bluetooth radio, Bluetooth sensor, Wi-Fi radio, Wi-Fi sensor, occupancy sensor.	See Figure 1.
Air flow	Avoid blocking inlet and outlet air vent zones.	See Figure 2

Item	Description	Notes
Audio	Avoid blocking audio exit zone on rear of Surface Hub 2S 50".	See Figure 2.

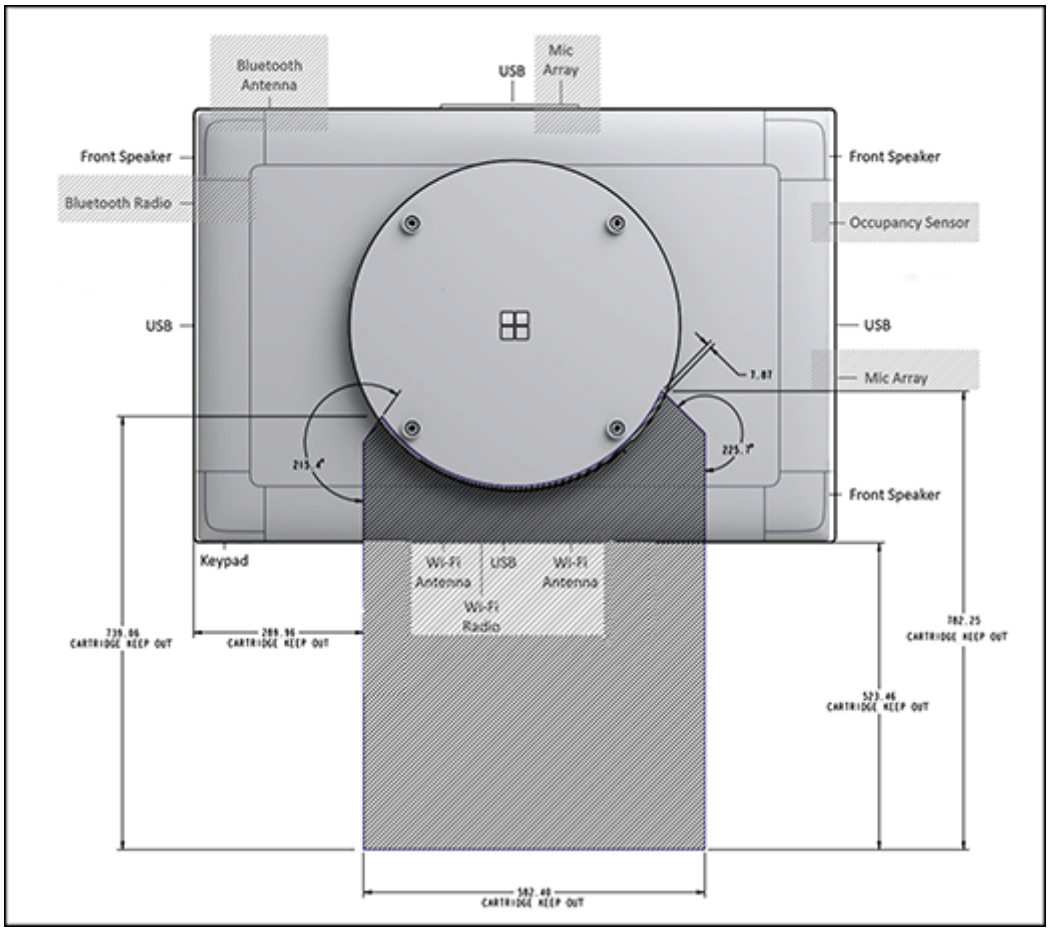


Figure 1. Keep out zones for Surface Hub 2S 50" components

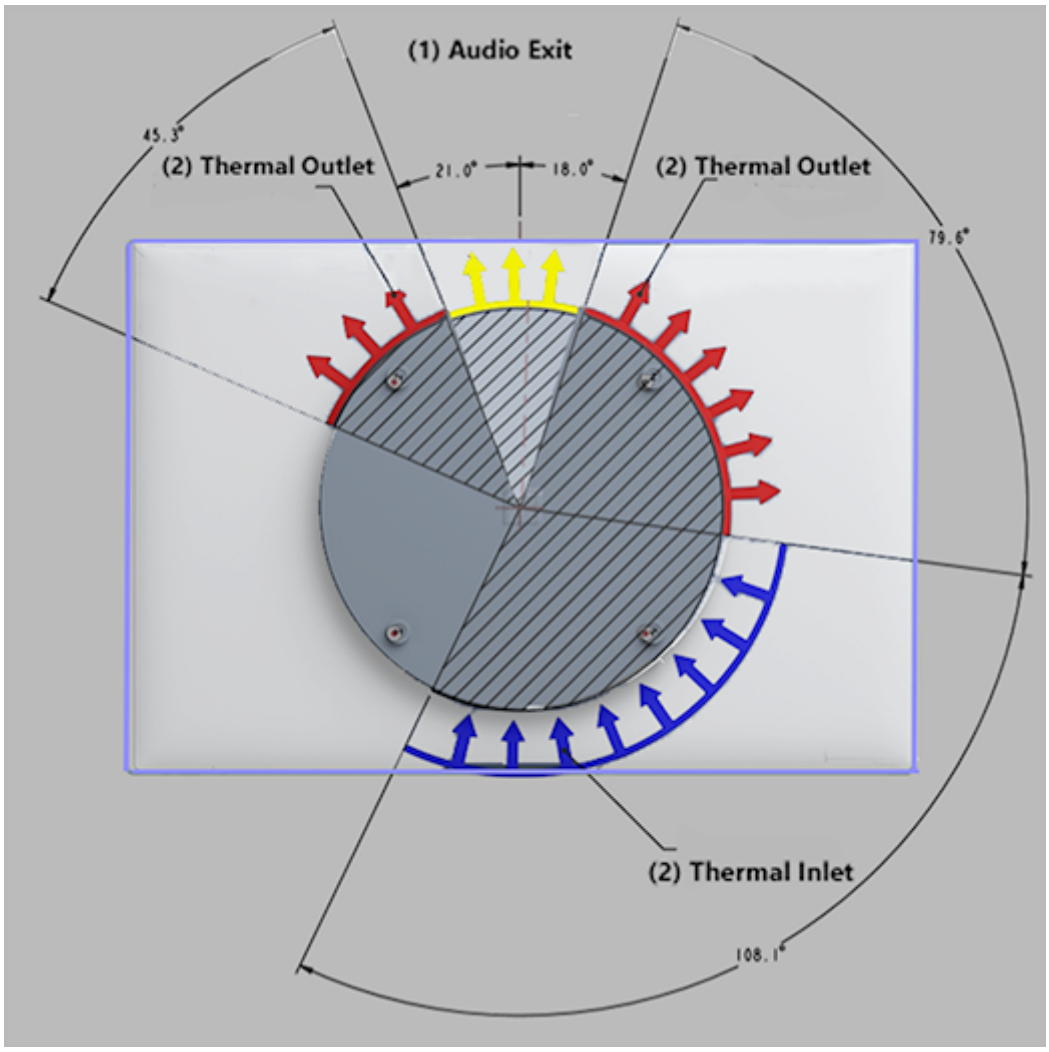


Figure 2. Avoid blocking thermal inlet/outlet and audio exit zones.

The removable compute cartridge containing the I/O ports must remain free of any obstructions or impediments of any kind.

Figure 3.View of compute cartridge on the underside of Surface Hub 2S 50".

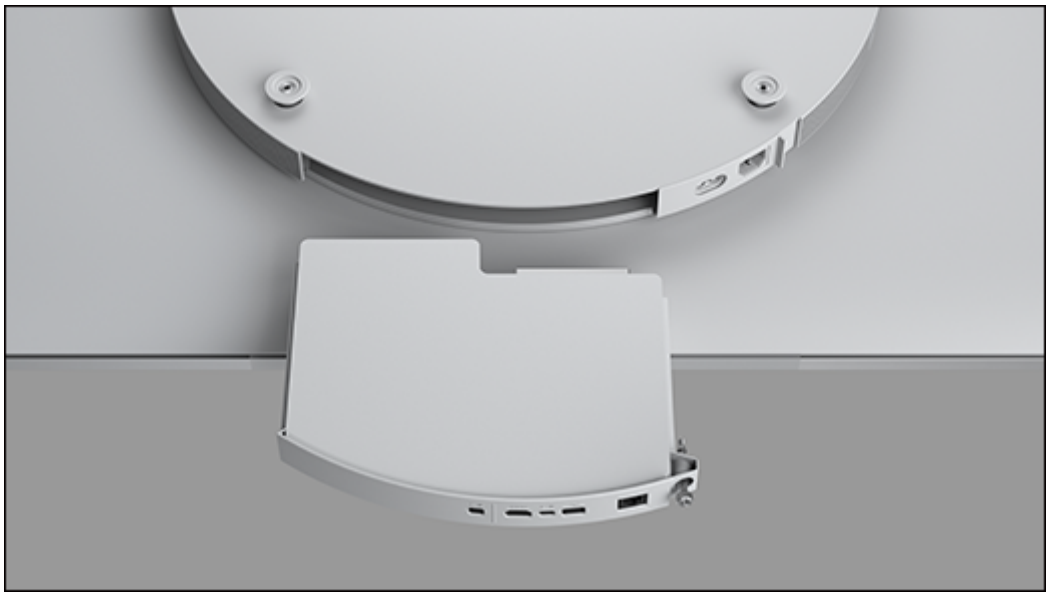


Figure 4. Unimpeded removal of compute cartridge

Selecting a mounting system

Surface Hub 2S 50" uses a 350 mm x 350 mm mounting framework that meets most — but not all — of the criteria listed in the VESA Flat Display Mounting Interface Standard. You can install Surface Hub 2S 50" using any of various off-the-shelf display brackets designed to accommodate displays that diverge from exact VESA specifications, as shown below.

On the back of Surface Hub 2S 50", you'll find a square pattern of four M6 x 1.0 threaded holes centered on the circular bump (565 mm in diameter). Attach your mount using four M6 x 1.0–12 mm-long metric bolts. Or, depending on preference, you can use longer bolts up to a maximum of 20 mm. Important considerations for mounting systems

Item	Description	Notes
Strength	Only choose mounts that can safely support devices of at least 28 kg (62 lbs.).	Required
Stiffness	Avoid flexible display mounts that can diminish the interactive pen and touch use experience. Most TV mounts are not designed to support touch displays.	Recommended
Depth	Keep the device mounted tightly to the wall especially in corridors and along circulation paths within rooms.	Recommended
Versatility	Ensure your mounting solution remains hidden from view in both the existing landscape mode and any potential portrait mode (subject to future availability).	Recommended

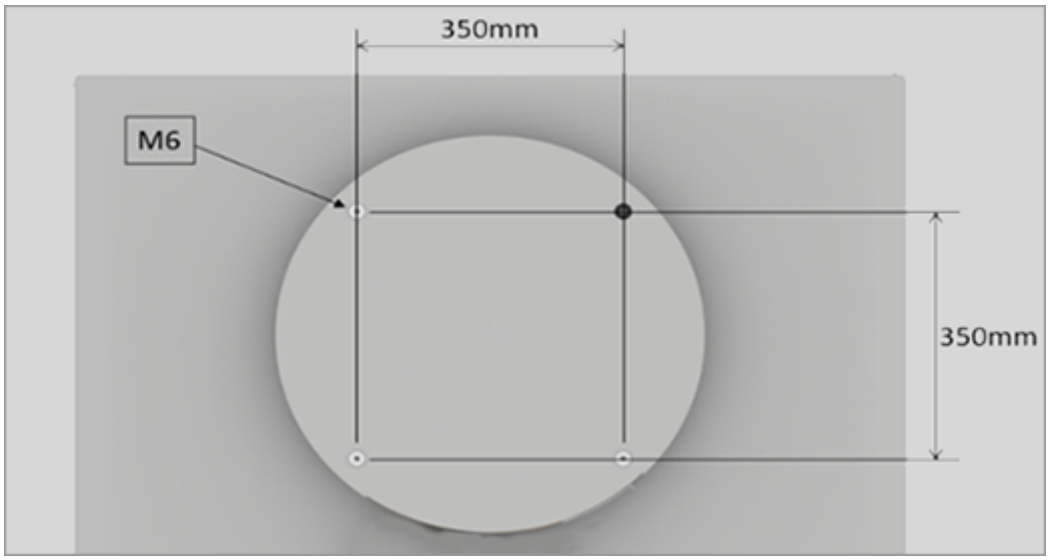


Figure 5. Surface Hub 2S 50" mounting configuration

Mounting methods compatible with Surface Hub 2S 50"

Surface Hub 2S 50" is compatible with mounts that allow you to place it at angles of 10-70 degrees from the vertical plane. Rail mounts typically have multiple holes and a set of slots, enabling compatibility across a wide range of displays. A rail attached to the wall and two mounts attached to the display enable you to securely install Surface Hub 2S 50" to a wall. When evaluating rail mounts for compatibility, ensure they meet versatility requirements listed earlier.

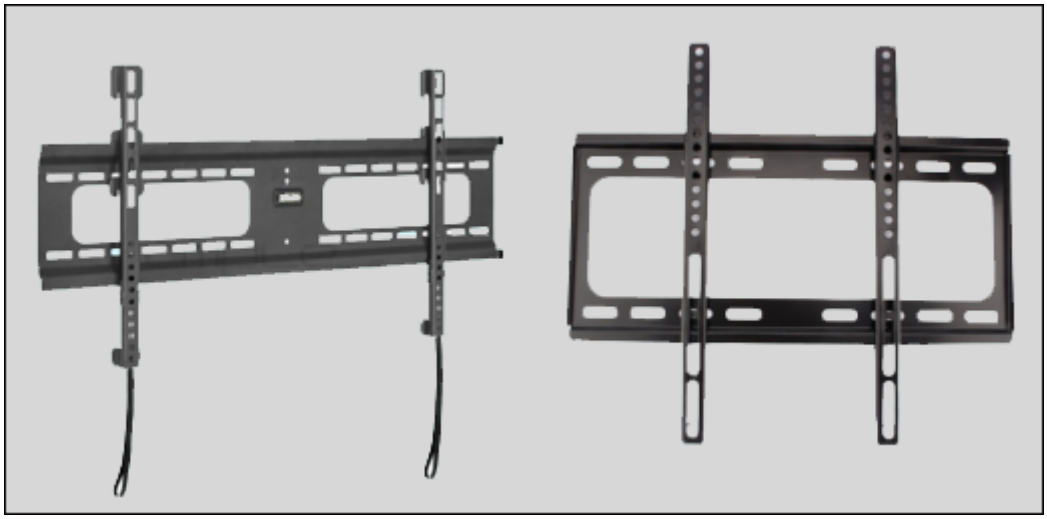


Figure 6. Surface Hub 2S 50" rail mounts

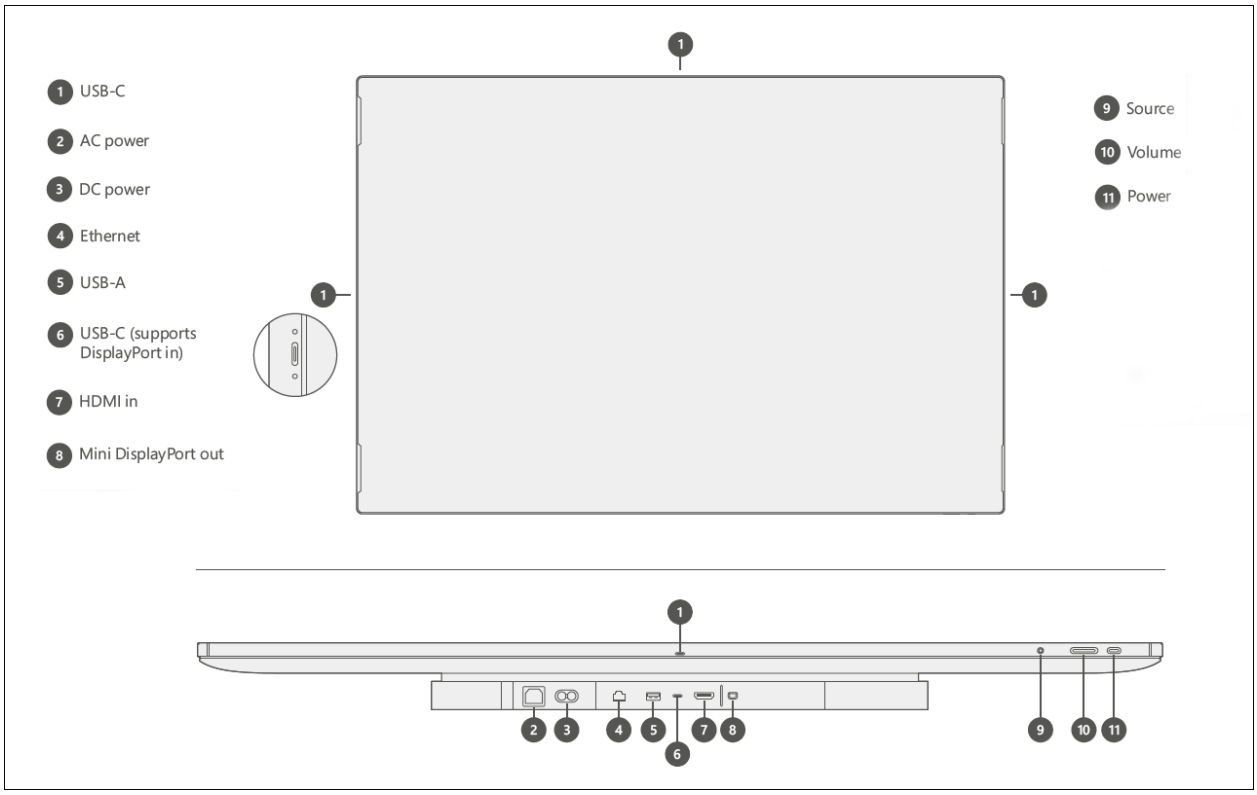
Surface Hub 2S ports and keypad overview

Article • 01/03/2023

This page describes the ports, physical buttons, and configuration information essential for connecting to Surface Hub 2S whether via wired, Wi-Fi, or Bluetooth methods. It also includes best practice recommendations for key connectivity scenarios.

> **Note**
>
> You can find the serial number on the outside of the packaging, on the display by the power cord, or by using the Surface app.

The figure below shows the location of ports and physical buttons on a keypad attached to the underside of the device. The table includes detailed descriptions of each element.

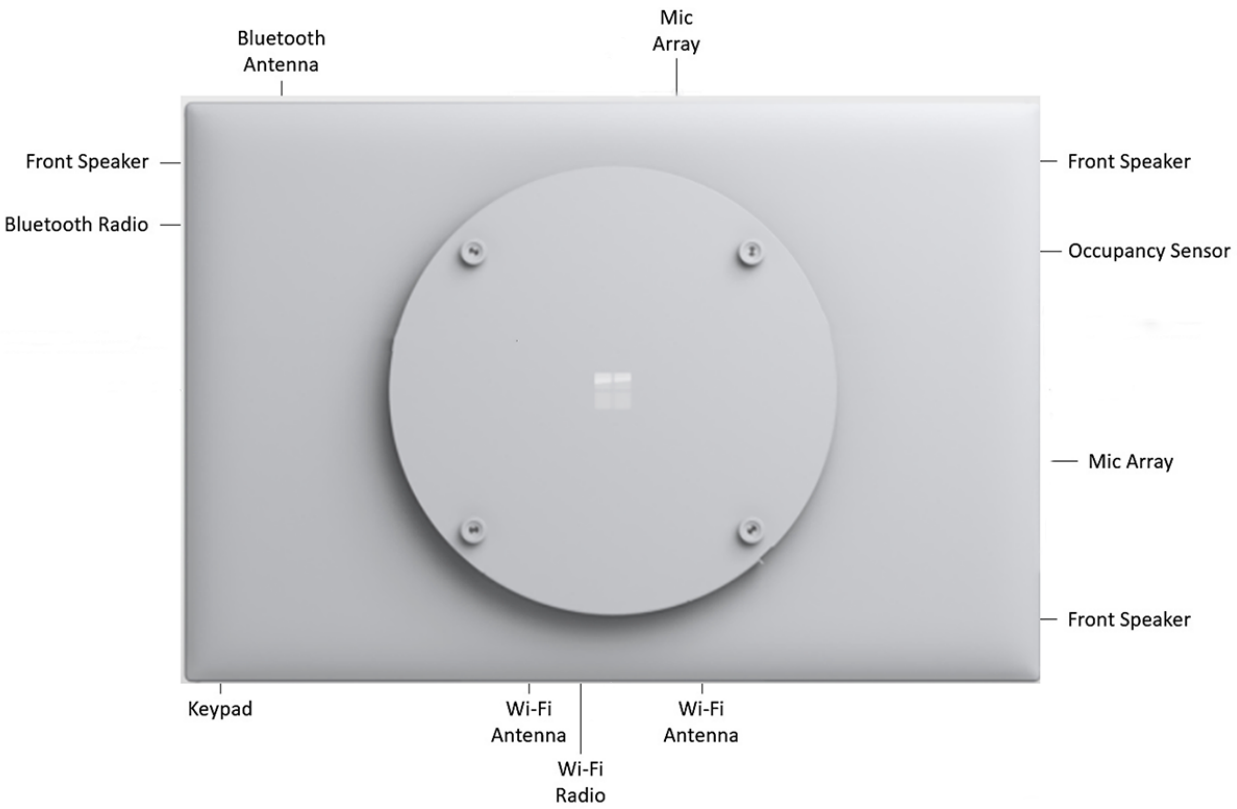


Port and keypad component reference

Key	Component	Description	Key parameters

Key	Component	Description	Key parameters
1	**USB C**	**USB 3.1 Gen 1** Use as a walk-up port for plugging in peripherals such as thumb-drives. Guest ports are on each side of the device (4). *NOTE: This is the recommended port for connecting an external camera. Additional camera mount features are incorporated into the design to help support retention of attached cameras.* NOTE: TouchBack and video ingest are not supported on these ports.	Type C 15 W Port (5V/3A)
2	**AC power**	**100-240 V input** Connect to standard AC power and Surface Hub 2S will auto switch to the local power standard such as110 volts in the US and Canada or 220 volts in the UK.	IEC 60320 C14
3	**DC power**	**24V DC input port** Use for connecting to mobile battery.	Xbox1 Dual barrel to Anderson connector
4	**Ethernet**	**1000/100/10 Base-T** Use for providing a continuous connection in a corporate environment and related scenarios requiring maximum stability or capacity.	RJ45
5	**USB-A**	**USB 3.1 Gen 1** Use as a walk-up port for plugging in peripherals such as thumb-drives.	Type A 7.5 W Port (5V/1.5A)
6	**USB-C**	**USB 3.1 Gen 1** Use as a walk-up port for connecting external PCs and related devices or plugging in peripherals such as thumb-drives. *NOTE: This is the recommended input port for video, TouchBack, and InkBack.*	Type C 18 W Port (5V/3A, 9V/2A)
7	**HDMI-in**	**HDMI 2.0, HDCP 2.2 /1.4** Use for multiple scenarios including HDMI-to-HDMI guest input.	Standard HDMI

Key	Component	Description	Key parameters
8	**Mini DP-out**	**Mini DP 1.2 output** Use for video-out scenarios such as mirroring the Surface Hub 2S display to a larger projector. *NOTE: This supports a maximum resolution of 3840 x 2160 (4K UHD) @60Hz.*	Mini DP
9	**Source**	Use to toggle among connected ingest sources — external PC, HDMI, and Mini DP modes.	n/a
10	**Volume**	Use +/- to adjust audio locally on the device. *NOTE: When navigating to the brightness control, use +/- on the volume slider to control display brightness.*	n/a
11	**Power**	Power device on/off. Use also to navigate display menus and select items.	n/a



Adjust Surface Hub 2S brightness, volume, and input

Article • 01/03/2023

Surface Hub 2S provides an on-screen display for volume, brightness, and input control. The Source button functions as a toggle key to switch between the volume, brightness, and input control menus.

To show the on-screen display

- Press and hold the **Source** button for 4 seconds.

When the on-screen display is visible, use one or more buttons to reach desired settings.

To adjust volume

- Use the **Volume up/down** button to increase or decrease volume.

To adjust brightness

1. Press the **Source** button again to switch to the brightness menu.
2. Use the **Volume up/down** button to increase or decrease brightness.

To adjust input

1. Press the **Source** button twice to switch to the Source menu.
2. Use the **Volume up/down** button to switch between PC, HDMI, and USB-C inputs.

Update pen firmware on Surface Hub 2S

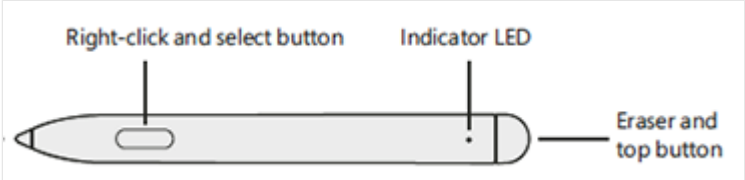
Article • 01/03/2023

You can update firmware on Surface Hub 2 pen from Windows Update for Business or by downloading the firmware update to a separate PC.

Update pen firmware using Windows Update for Business

This section describes how to update pen firmware via the automated maintenance cycles for Windows Update, configured by default to occur nightly at 3 a.m. You will need to plan for two maintenance cycles to complete before applying the update to the Surface Hub 2 pen. Alternately, like any other update, you can use Windows Update for Business (WUfB) to apply the pen firmware. For more information, see Managing Windows updates on Surface Hub.

1. Ensure the Surface Hub 2 pen is paired to Surface Hub 2S: Press and hold the **top** button until the white indicator LED light begins to blink.



2. On Surface Hub, login as an Admin, open **Settings**, and then scan for new Bluetooth devices.

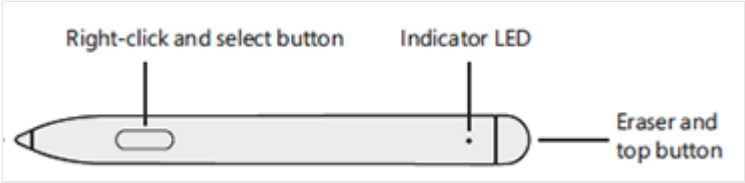
3. Select the pen to complete the pairing process.

4. Press the **top** button on the pen to apply the update. It may take up to two hours to complete.

Update pen firmware by downloading to separate PC

You can update the firmware on Surface Hub 2 pen from a separate PC running Windows 10 or Windows 11. This method also enables you to verify that the pen firmware has successfully updated to the latest version.

1. Pair the Surface Hub 2 pen to your Bluetooth-capable PC: Press and hold the **top** button until the white indicator LED light begins to blink.



2. On the PC, scan for new Bluetooth devices.
3. Select the pen to complete the pairing process.
4. Disconnect all other Surface Hub 2s pens before starting a new update.
5. Download the Surface Hub 2 Pen Firmware Update Tool to your PC.
6. Run **PenCfu.exe.** The install progress is displayed in the tool. It may take several minutes to finish updating.

Check firmware version of Surface Hub 2 pen

1. Run **get_version.bat** and press the **top** button on the pen.
2. The tool will report the firmware version of the pen.

   Example:

   - Old firmware is 468.2727.368
   - New firmware is 468.3347.368

Command line options

You can run Surface Hub 2 Pen Firmware Update Tool (PenCfu.exe) from the command line.

1. Pair the pen to your PC and click the **top** button on the pen.
2. Double click **PenCfu.exe** to initiate the firmware update. Note that the configuration file and the firmware image files must be stored in the same folder as the tool.
3. For additional options, run **PenCfu.exe -h** to display the available parameters, as listed in the following table. Example: `PenCfu.exe -h`
4. Enter **Ctrl+C** to safely shut down the tool.

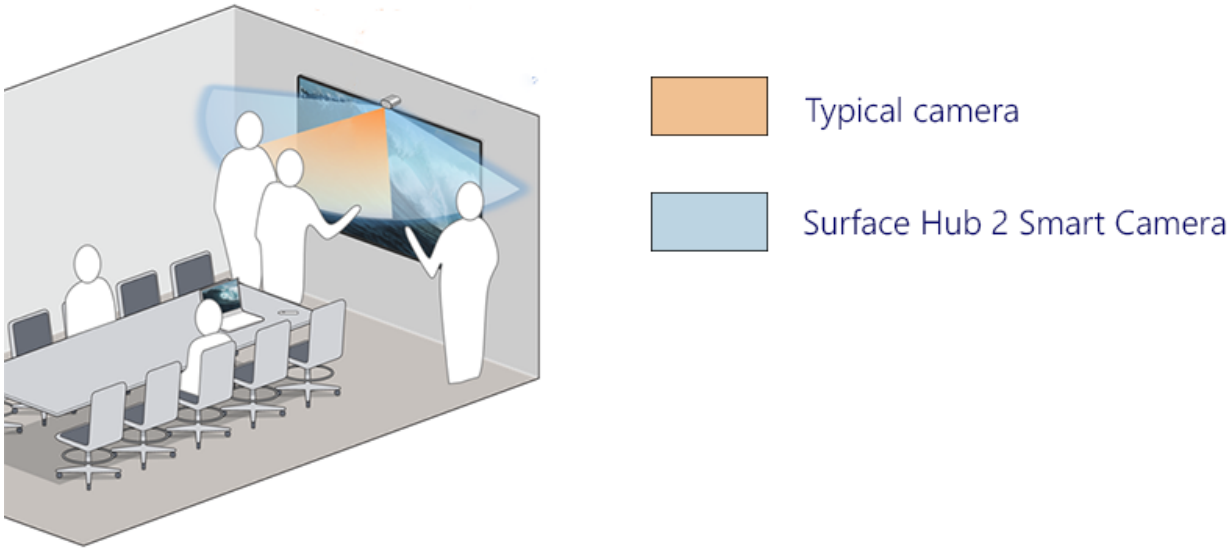
Command	Description

Command	Description
-h help	Display tool command line interface help and exit.
-v version	Display tool version and exit.
-l log-filter	Set a filter level for the log file. Log messages have 4 possible levels: DEBUG (lowest), INFO, WARNING and ERROR (highest). Setting a log filter level filters log messages to only message with the same level or higher. For example, if the filter level is set to WARNING, only WARNING and ERROR messages will be logged. By default, this option is set to OFF, which disables logging.
-g get-version	If specified, the tool will only get the FW version of the connected pen that matches the configuration file that is stored in the same folder as the tool.

Install and Manage Surface Hub 2 Smart Camera

Article • 01/03/2023

Surface Hub 2 Smart Camera[1] is designed for hybrid teams and optimized for remote participants. With a sharp focus on the foreground and background, remote participants can see people interact with content on the Surface Hub while also viewing everyone else in the room. Surface Hub 2 Smart Camera has a wide field of view greater than 136 degrees, automatic framing, high-quality glass optics, and a low light sensor.



Ultra-wide camera view includes people whiteboarding on extreme edges of 85" Hub

System requirements

For Surface Hubs running Team OS, Surface Hub 2 Smart Camera requires the following updates for the Windows 10 Team 2020 update (20H2) on Surface Hub 2:

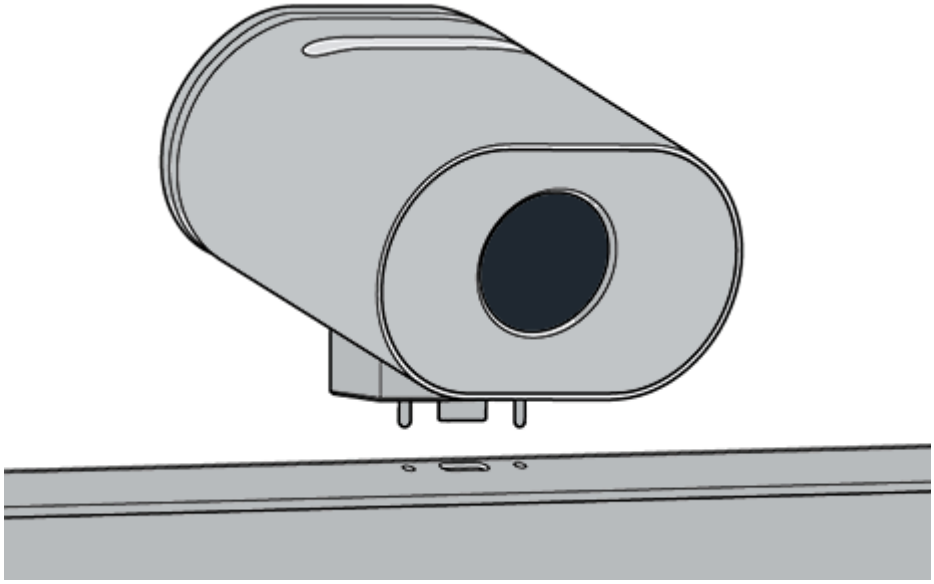
- Windows 10 Team 2020 Update 2 (KB5010415 or a subsequent Windows update)
- System Hardware Update-January 21, 2022 (or a subsequent System Hardware Update)

To learn more, refer to Surface Hub update history.

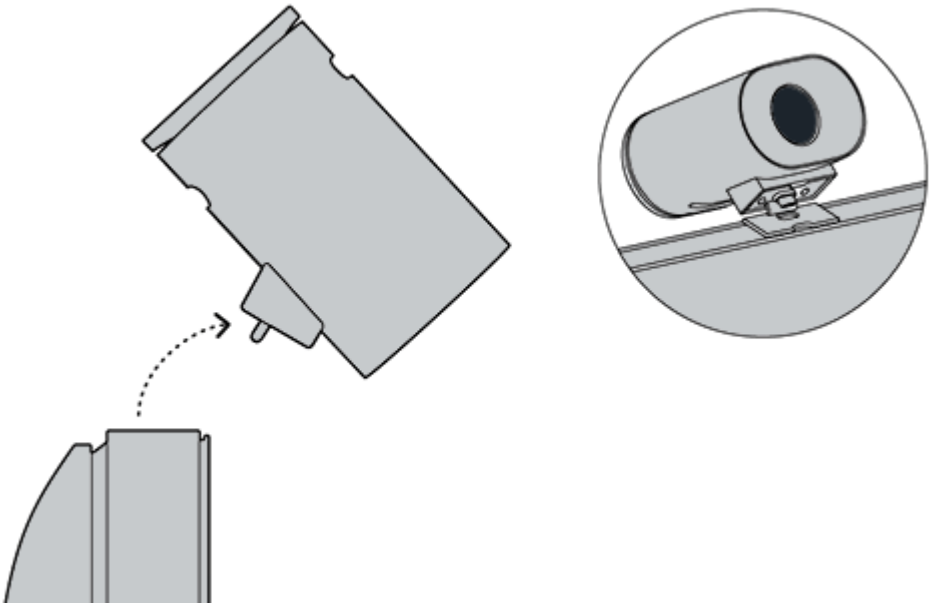
> **Note**
>
> No additional updates are required for Surface Hubs migrated to run Windows 10/11 Pro or Enterprise.

Install smart camera

1. Attach the camera to the USB-C port in the middle of the top of Surface Hub 2. The indicator LED will light briefly when the camera is connected and continuously when the camera is in use.

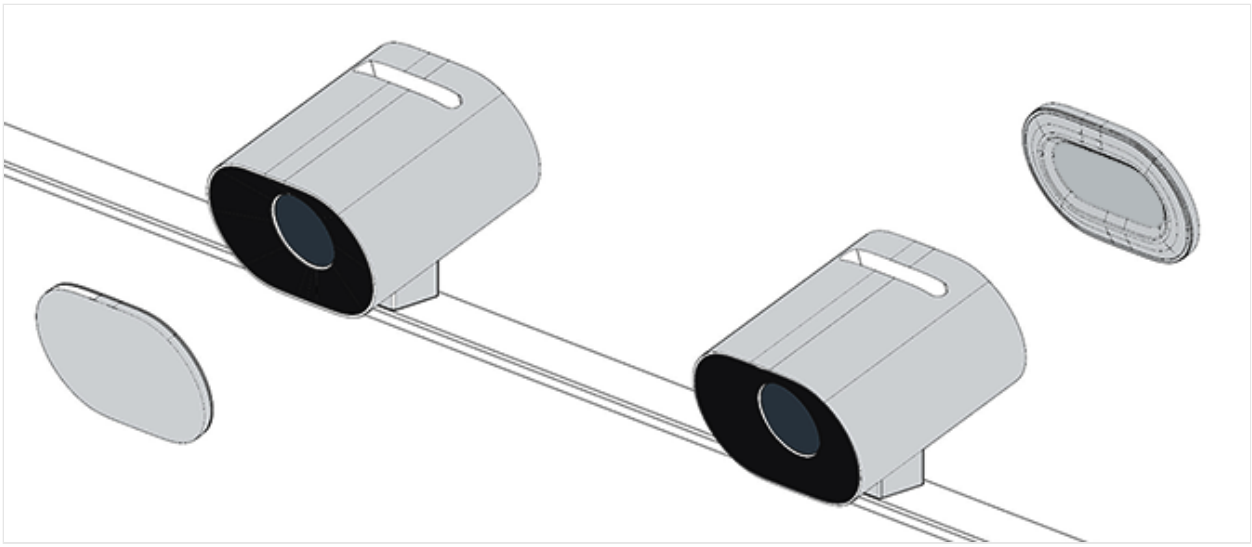


2. To remove the camera, pull up and forward. A magnetic tether prevents the camera from being knocked off or pulled backward.



Camera cover

The camera cover magnetically snaps to the front for privacy and the back for storage when not in use.



> **Note**
>
> Do not place the cover in the vented slot at the top of the camera.

Manage automatic framing settings

Automatic framing dynamically zooms and keeps you centered in the video when you move around. How you manage the settings depends on the OS installed on Surface Hub:

- Windows 10 Team 2020 update (20H2)
- Windows 11 Desktop on Surface Hub
- Windows 10 Desktop on Surface Hub

Windows 10 Team 2020 update (20H2)

When you install the Surface Hub Smart Camera, automatic framing is enabled by default. Admins can manage automatic framing from Settings via an On/Off toggle that sets the automatic framing state at the start of each Surface Hub session.

To adjust automatic framing:

1. On your Surface Hub 2S, sign in as **Admin**.

> **Note**
>
> If you don't know your user name or admin password, you'll need to reset the device. For more information, see **Reset and recovery for Surface Hub 2S**.

2. Open **Settings** and go to **Surface Hub** > **Calling & Audio.**
3. Under **Automatic framing**, adjust the toggle as appropriate.
4. Select **End session**; modified settings are applied when you start a new session.

If the toggle is set to **On**, automatic framing will always be on by default when users begin a session on Surface Hub. If the toggle is set to **Off**, automatic framing will always be off by default when starting a session on Surface Hub.

Manage camera settings via an MDM provider

Admins can manage automatic framing via the Surface Hub configuration service provider (CSP) from Intune or a third-party mobile device management (MDM) provider.

CSP policy setting	Description
DefaultAutomaticFraming	If you turn on this policy setting, automatic framing is enabled. If you turn off this policy setting, automatic framing is disabled. If you don't configure this policy setting, automatic framing is enabled.

To learn more, refer to the following pages:

- Manage settings with an MDM provider
- SurfaceHub CSP - Windows Client Management

Windows 11 Desktop on Surface Hub

If you've migrated your Surface Hub to run Windows 11 Pro or Windows 11 Enterprise, you'll need to turn on automatic framing for the Surface Hub Smart Camera. By default, automatic framing is turned off.

To turn on automatic framing, go to **Settings** > **Bluetooth & devices** > **Manage Cameras**> **Surface Hub 2 Smart Camera.**

Windows 10 Desktop on Surface Hub

Automatic framing is always enabled and can't be disabled or otherwise configured.

Order Surface Hub 2 Smart Camera

Purchase Surface Hub 2 Smart Camera from your authorized Microsoft Surface reseller.

Learn more

-Video: The new Surface Hub 2 Smart Camera

References

[1] Surface Hub 2 Smart Camera, sold separately starting March 16, 2022, dynamically adjusts the video feed for remote participants. Surface Hub 2 Smart Camera will be included in the box with Surface Hub 2S 85" starting in May 2022.

Essential add-ons for Windows 10/11 Pro and Enterprise on Surface Hub 2

Article • 01/03/2023

If you have migrated from Windows 10 Team to Windows 10 or Windows 11 Pro or Enterprise on Surface Hub 2, you can choose from a wide variety of accessories that connect via USB-C, USB-A, HDMI, or Bluetooth.

Surface Hub 2 Fingerprint Reader

If you're running Windows 10/11 Pro or Windows 10/11 Enterprise on Surface Hub 2, you can sign in using the optional Surface Hub 2 Fingerprint Reader, a biometric authentication option that uses Windows Hello.

Ordering

Commercial customers can place orders through their Surface Authorized Device Resellers.

To use Surface Hub 2 Fingerprint Reader:

1. Insert the fingerprint reader into any of the USB C bezel ports, located on each side of the device.
2. **Go to Start** > **Settings** > **Accounts** > **Sign-in options** > **Windows Hello Fingerprint** to enroll your fingerprint.

For more information about configuring the fingerprint reader to sign in using Windows Hello, see the following:

- Learn about Windows Hello and set it up
- Windows Hello biometrics in the enterprise.

Table 1. Surface Hub 2 Fingerprint Reader tech specs

Component	Description
USB	Customized USB Type-C
System requirement	Windows 10/11 Pro, Windows 10/11 Enterprise.

Component	Description
Windows certification	Windows 10/11
False Acceptance Rate (FAR)	1/1.5 million. FAR shows the probability of a biometric security system to incorrectly accept access attempts by unauthorized users.
False Rejection Rate (FRR)	4.9%. FRR shows the probability of a biometric security system to incorrectly reject access attempts by authorized users.

> **Note**
>
> Windows 10 Team, which runs on Surface Hub 2S does not support the Surface Hub 2 Fingerprint Reader. This is because Windows 10 Team is designed to allow multiple users to interact with the device in a conference room environment.

Windows Hello face recognition

Windows 10/11 Pro and Enterprise on Surface Hub 2 supports Windows Hello for authentication and requires a Windows Hello certified camera accessory. Note that the built-in camera for Surface Hub 2S is not designed for authentication and does not support Windows Hello. For more information, see Windows Hello.

Audio and video accessories

You can extend the audio and video capabilities of Surface Hub 2 with audio and camera peripherals using the USB-C or USB-A ports.

For information about recommended accessories, see:

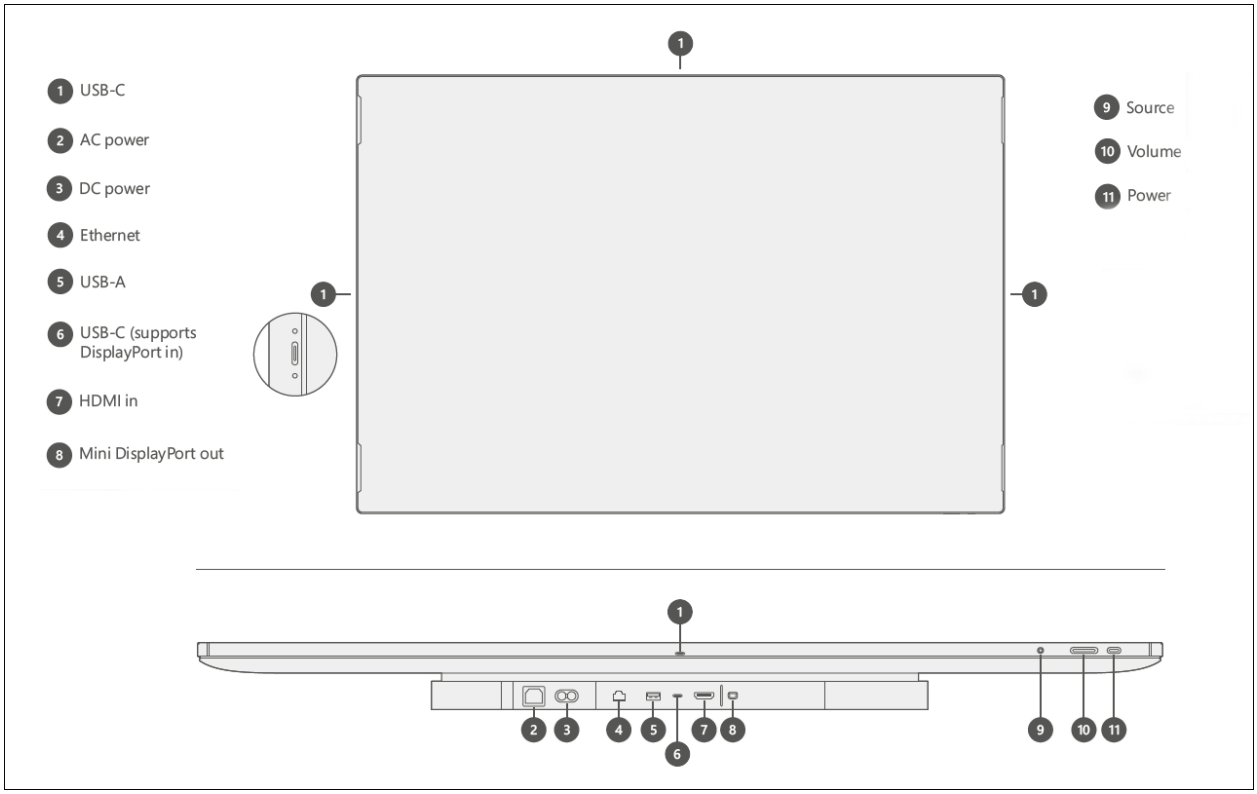
- USB audio and video devices certified for Microsoft Teams
- IP Phones certified for Microsoft Teams

Other accessories

Surface Hub 2 includes the following ports for connecting a wide variety of devices.

- 1 x USB A port on compute module (behind display)
- 4 x USB C ports on bezels
- Bluetooth 4.1 support

- HDMI 2.0



For more information, see Surface Hub 2S ports and keypad overview

Learn more

- Configure Windows 10/11 Pro or Enterprise on Surface Hub 2.

Microsoft Teams certified audio and video accessories for Surface Hub 2S

Article • 01/03/2023

Surface Hub 2S 50" and 85" models are certified for Microsoft Teams as all-in-one devices in huddle and collaboration spaces, at 2.3 meters and 3.5 meters respectively. The Surface Hub 2S family can be extended to larger rooms with the following tested and approved Microsoft Teams certified peripherals that bring the most out of any space when combined with Surface Hub 2S 50" and 85".

Microsoft Teams certified audio accessories

Model	Description
Yamaha YVC-1000MS	For up to six participants. - Use one to five expansion mics for Microsoft Teams certification in rooms with up to 40 participants.
Sennheiser EXPAND SP 20	For up to six participants. Microsoft Teams certified.
Yealink CP900	For up to six participants. Microsoft Teams certified.

Microsoft Teams certified video accessories

Model	Description
Surface Hub 2 Smart Camera	4K, 136 degrees, digital PTZ (pan-tilt-zoom) Up to 8 meters for video subjects
Jabra PanaCast	4K, 180 degrees. Up to 3 meters for video subjects
Poly Studio - Huddle Room USB Video Bar	4K, 120 degrees Up to 3.7 meters for audio + video subjects
Polycom EagleEye Director II	1080p, 65 degrees 10+ participants medium rooms
Logitech Rally Bar	4K, 90 degrees, PTZ, manual/digital control, USB 3.0 Type-C, privacy assurance

Learn more

- Meeting Room Systems, VoIP Phones, Headsets | Microsoft Teams

Reset and recovery for Surface Hub 2S

Article • 01/10/2023 • Applies to: Surface Hub 2S

If you encounter problems with Surface Hub 2S, you can reset the device to factory settings or restore using a USB drive.

To begin, sign in to Surface Hub 2S with admin credentials, open the **Settings** app, select **Update & security**, and then select **Recovery**.

Reset the device

> **Important**
>
> Ensure that you have your BitLocker key available before resetting the device, as you will be prompted for it later. To learn more, see **Save your BitLocker key**.

1. To reset the device, select **Get Started**.
2. When the **Ready to reset this device** window appears, select **Reset**.

   > **Tip**
   >
   > When the Hub reboots to the recovery partition, it will prompt you to enter the BitLocker key. Skipping that prompt will cause the reset to fail. Once you enter the BitLocker key, the Hub reinstalls the operating system from the recovery partition. This may take up to one hour to complete.

3. To reconfigure the device, run the first-time Setup program.
4. If you manage the device using Microsoft Intune or another mobile device management solution, retire and delete the previous record, and then re-enroll the new device. For more information, see Remove devices by using wipe, retire, or manually unenrolling the device.

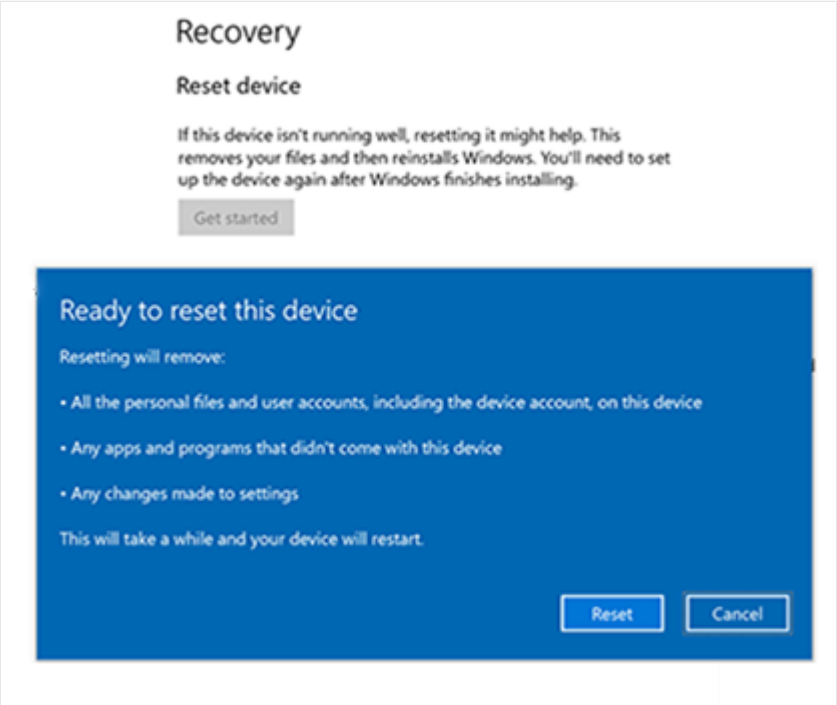


Figure 1. Reset and recovery for Surface Hub 2S

Recover Surface Hub 2S by using a USB recovery drive

New in Surface Hub 2S, you can now reinstall the device by using a recovery image.

Recovery from a USB drive

Using Surface Hub 2S, you can reinstall the device using a recovery image. By doing this, you can reinstall the device to the factory settings if you lost the BitLocker key or if you no longer have admin credentials to the Settings app.

> **Tip**
>
> Use a USB 3.0 drive with 16 GB or 32 GB of storage, formatted as FAT32.

1. From a separate PC, download the .zip file recovery image from the Surface Recovery website and then return to these instructions.
2. In the search box on the taskbar, enter **recovery drive**, and select **Create a recovery drive** or **Recovery Drive** from the results. You may need to enter an admin password or confirm your choice.
3. In the **User Account Control** box, select **Yes**.

4. Make sure to clear the **Back up system files to the recovery drive** check box and then select **Next**.
5. Select your USB drive, and then select **Next** > **Create**. Some utilities need to be copied to the recovery drive, so this might take a few minutes.
6. When the recovery drive is ready, select **Finish**.
7. Double-click the recovery image .zip file that you previously downloaded to open it.
8. Select all the files from the recovery image folder, copy them to the root of your USB drive, and then select **Choose to replace the files in the destination**.
9. Once the files have finished copying, select the **Safely Remove Hardware and Eject Media** icon on the taskbar and remove your USB drive.
10. Connect the USB drive to any USB-C or USB-A port on the Surface Hub 2S. Turn off the Hub and then boot from the USB drive.

Boot Surface Hub from USB drive

> ⓘ **Note**
>
> If the device was unplugged or experienced an abrupt power outage or pulled power cord, wait at least 15 seconds before attempting to boot from USB.

1. While pressing the Volume down button, press the Power button.
2. Keep pressing both buttons until you see the Windows logo.
3. Release the Power button but continue to hold the Volume down button until the Install UI begins.

Figure 2. Volume and Power buttons

4. On the language selection screen, select the display language for your Surface Hub 2S.

5. Select **Recover from a drive** and **Fully clean the drive**, and then select **Recover**. If you're prompted for a BitLocker key, select **Skip this drive**. Surface Hub 2S reboots several times and can take an hour or more to complete the recovery process.

6. When the first-time setup screen appears, remove the USB drive.

Troubleshooting and common problems

Issue	Notes
Unable to download recovery image from the Surface Recovery website	Try downloading it on another network; ideally, a standalone device, not joined to a domain, with open access to the internet (no proxies).
You're prompted for a recovery key	Select the option to **Skip this drive.**
BMR fails at 99% or X%	Check the following potential issues: - **Connections.** Ensure your USB drive is directly connected to the USB port in the compute cartridge, located on the rear of Surface Hub 2S. Remove any in-between cables that may be in use. - **Storage space.** Ensure your USB drive has enough space for the image (the BMR image might occupy more space on the drive than the actual available size). - **Damaged recovery image.** Try recreating the image using the precise steps listed above to ensure it wasn't damaged during installation. - **Possible hardware failure.** If available, try installing your USB drive on another Surface Hub and see if you can successfully boot to the drive. If so, this might indicate a hardware failure, which will require opening a support case.
Preparing automatic repair not showing	- Check that you followed these steps, exactly as shown in the previous section, Boot Surface Hub from USB drive, and repeated here: 1. While pressing the Volume down button, press the Power button. 2. Keep pressing both buttons until you see the Windows logo. 3. Release the Power button but continue to hold the Volume down button until the Install UI begins. - **Test on another Surface Hub.** If available, try installing your USB drive on another Surface Hub and see if you can successfully boot to the drive. If so, this might indicate a hardware failure, which will require opening a support case.

Issue	Notes
USB isn't recognized	- **Check image**. Ensure the image is created correctly. All recovery image files must be extracted from the original .ZIP file and be saved to the root of your USB drive [the root is the top level of your USB drive]. - **Check USB format.** Confirm you're using a supported USB drive. It must be a USB 3.0 drive with 16 GB or 32 GB of storage, formatted as FAT32. You can check if a laptop recognizes the USB and that the BMR image is present. - If the USB drive is formatted correctly but still not working, try using a different USB brand. - Use a USB-C flash drive instead and start the process from the beginning. - Double-check you completed the following step, as shown earlier in **Step 10** from Recovery from a USB drive, and repeated here: Connect the USB drive to any USB-C or USB-A port on the Surface Hub 2S. Turn off the Hub and then boot from the USB drive. Try connecting to another USB-C or USB-A port on Surface Hub 2S.

Contact Support

If you have questions or need help, you can create a support request.

Troubleshoot Surface Hub 2S power issues

Article • 01/03/2023 • Applies to: Surface Hub 2S

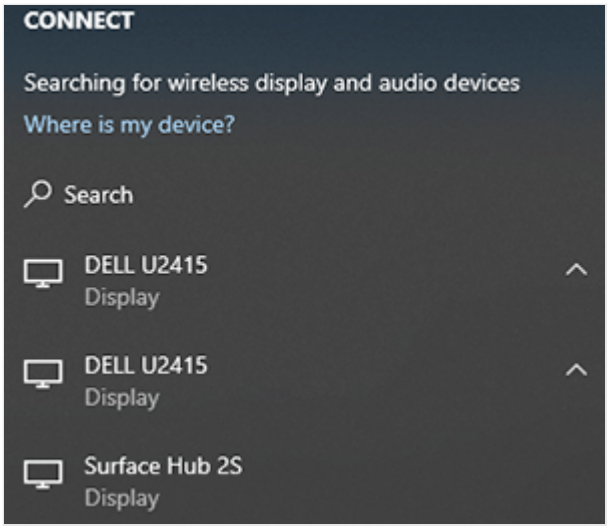
If you encounter an issue powering on your Surface Hub 2S, review the troubleshooting steps outlined on this page.

1. First, remove all connections to the Surface Hub 2S except for Ethernet and power.
2. Ensure Surface Hub 2S has a direct connection to a dedicated power outlet.
3. Do you have an APC Charge Mobile Battery connected to Surface Hub? If yes, disconnect the battery and try again. If the power-on issue only occurs when using the APC battery, please contact APC support for further assistance.
4. Test with another power cord (see Label 2 in Figure 1 below) and a different power outlet.
5. Initiate a hardware reset on Surface Hub 2S: Hold and press the power button (see Label 11 in Figure 1 below) for at least 20 seconds.
6. If you're still unable to power on the device, try reseating the compute cartridge.

Support requests

If your Surface Hub 2S still fails to power on after trying these troubleshooting steps, please create a support request and include the following details:

- Results of your troubleshooting steps.
- Is the backlight visible on the device?
- Can you use the Source button on the keypad to select other sources? (To locate the Source button, see Label 9 in Figure 1 below). Are the sources visible on the screen?
- If you try to connect an external device (via HDMI, for example), does the Hub display the external content?
- If you Miracast to the Surface Hub from a projecting device, does the Surface Hub appear as an available connection, as shown below?



- Date of Surface Hub 2S delivery and discovery of the unresponsive unit.
- The serial number of the Surface Hub 2S.

> **Tip**
>
> The serial number is printed on Surface Hub 2S near the power cord, as shown below.

Port and keypad component reference

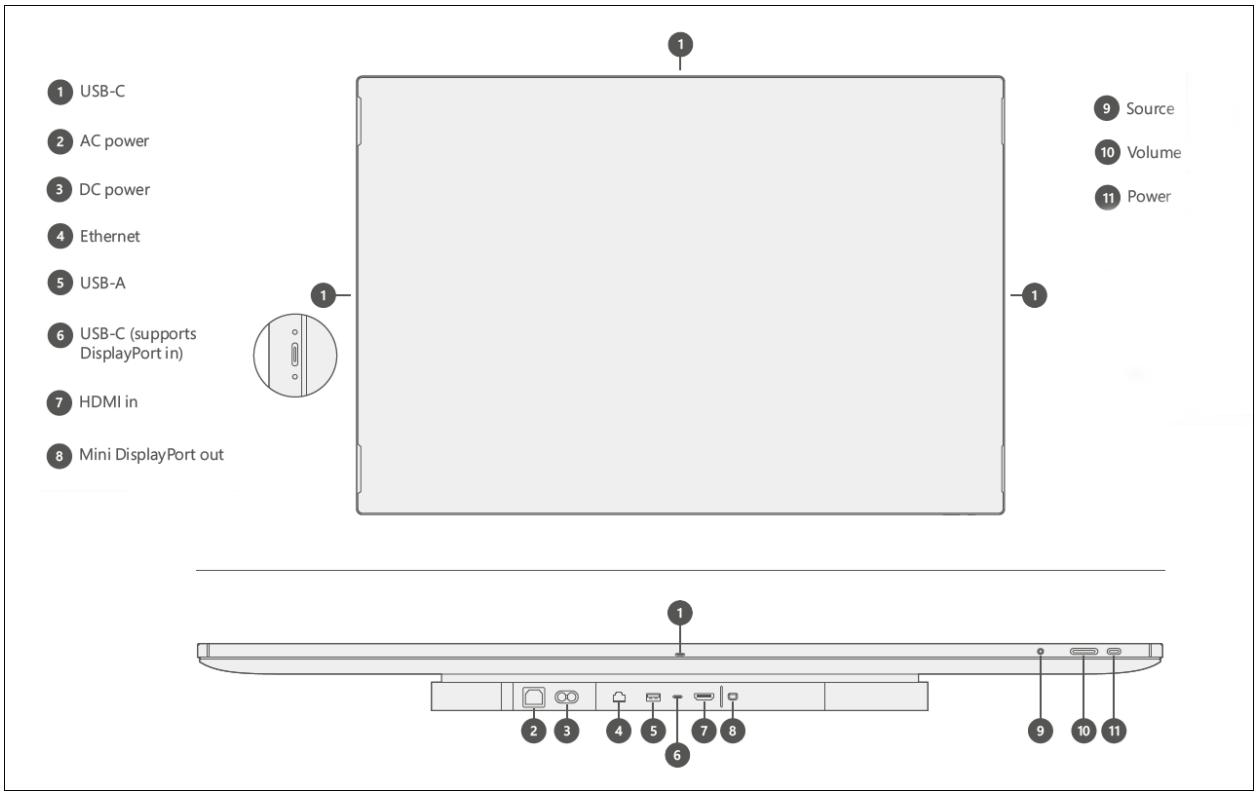


Figure 1. Ports and physical buttons on Surface Hub 2S

Key	Component	Description	Key parameters
1	**USB C**	**USB 3.1 Gen 1** Use as a walk-up port for plugging in peripherals such as thumb-drives. Guest ports are on each side of the device (4). *NOTE: This is the recommended port for connecting an external camera. Additional camera mount features are incorporated into the design to help support retention of attached cameras.* NOTE: TouchBack and video ingest are not supported on these ports.	Type C 15 W Port (5V/3A)
2	**AC power**	**100-240 V input** Connect to standard AC power and Surface Hub 2S will auto switch to the local power standard such as110 volts in the US and Canada or 220 volts in the UK.	IEC 60320 C14
3	**DC power**	**24V DC input port** Use for connecting to mobile battery.	Xbox1 Dual barrel to Anderson connector

Key	Component	Description	Key parameters
4	**Ethernet**	**1000/100/10 Base-T** Use for providing a continuous connection in a corporate environment and related scenarios requiring maximum stability or capacity.	RJ45
5	**USB-A**	**USB 3.1 Gen 1** Use as a walk-up port for plugging in peripherals such as thumb-drives.	Type A 7.5 W Port (5V/1.5A)
6	**USB-C**	**USB 3.1 Gen 1** Use as a walk-up port for connecting external PCs and related devices or plugging in peripherals such as thumb-drives. *NOTE: This is the recommended input port for video, TouchBack, and InkBack.*	Type C 18 W Port (5V/3A, 9V/2A)
7	**HDMI-in**	**HDMI 2.0, HDCP 2.2 /1.4** Use for multiple scenarios including HDMI-to-HDMI guest input.	Standard HDMI
8	**Mini DP-out**	**Mini DP 1.2 output** Use for video-out scenarios such as mirroring the Surface Hub 2S display to a larger projector. *NOTE: This supports a maximum resolution of 3840 x 2160 (4K UHD) @60Hz.*	Mini DP
9	**Source**	Use to toggle among connected ingest sources — external PC, HDMI, and Mini DP modes.	n/a
10	**Volume**	Use +/- to adjust audio locally on the device. *NOTE: When navigating to the brightness control, use +/- on the volume slider to control display brightness.*	n/a
11	**Power**	Power device on/off. Use also to navigate display menus and select items.	n/a

Troubleshoot APC Charge Mobile Battery on Surface Hub 2S

Article • 01/30/2023

The APC Charge Mobile Battery lets you move your Surface Hub 2S for unplugged and uninterrupted teamwork capabilities. If Surface Hub 2S won't power on when connected to the APC Charge Mobile Battery, try the troubleshooting steps on this page.

A. Verify that all connections between the Surface Hub 2S and the APC Charge Mobile Battery are **securely and adequately seated.**

Connections include the following items, as shown in Figure 1.

1. USB cable for onscreen battery display
2. DC cable for on-battery operation
3. AC passthrough cable for normal operation
4. AC power cord (supplied with Surface Hub 2S)

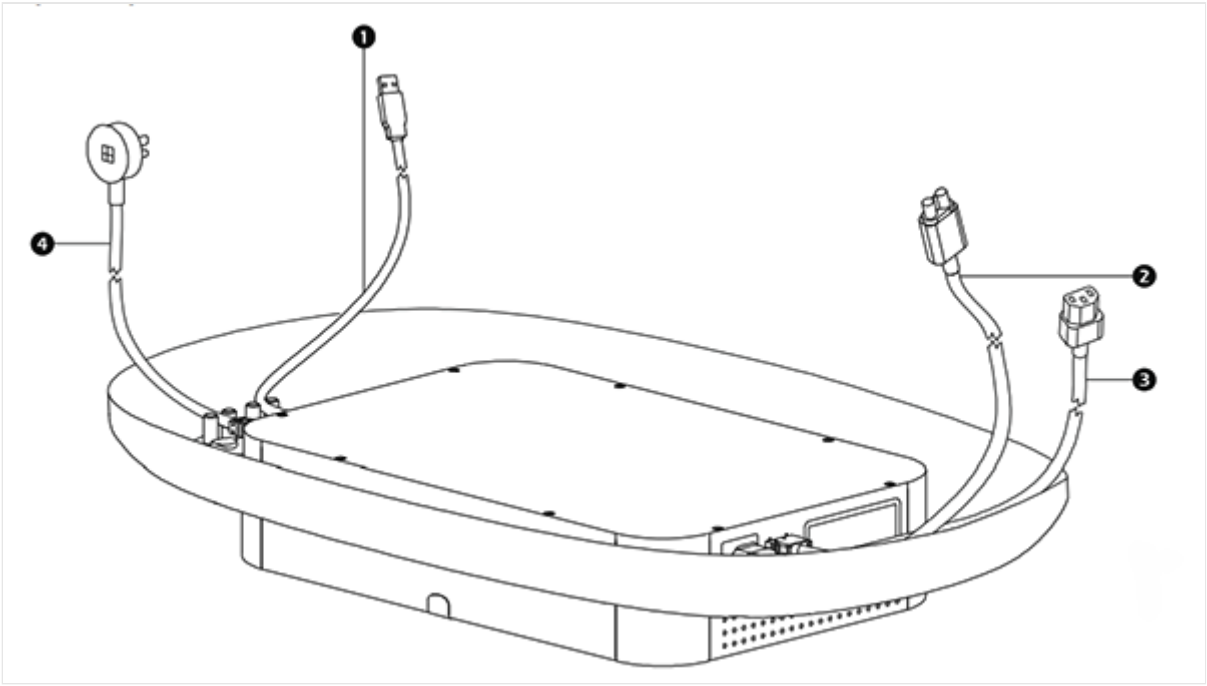


Figure 1. Input/output connections

The following figure shows the correct configuration:

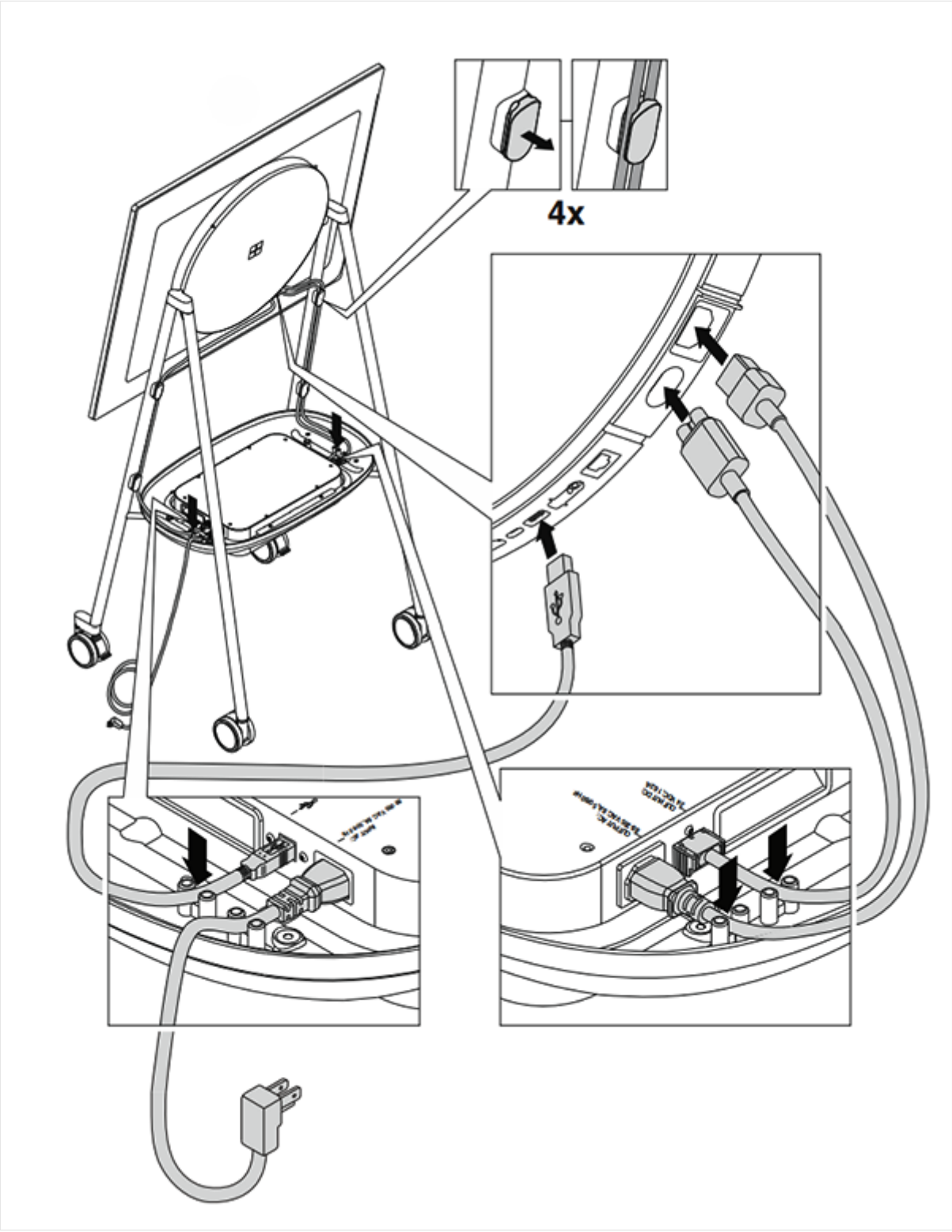


Figure 2. Correct configuration of input/output connections

> ⓘ **Note**
>
> To learn more, refer to the **APC Charge Mobile Power Supply User Manual** .

B. Ensure that the APC Charge Mobile Battery is powered on by pressing the **power on/off** button for more than 3 seconds and less than 6 seconds to enable the 24 V DC output voltage. The LEDs will turn white to indicate the battery's charge state.

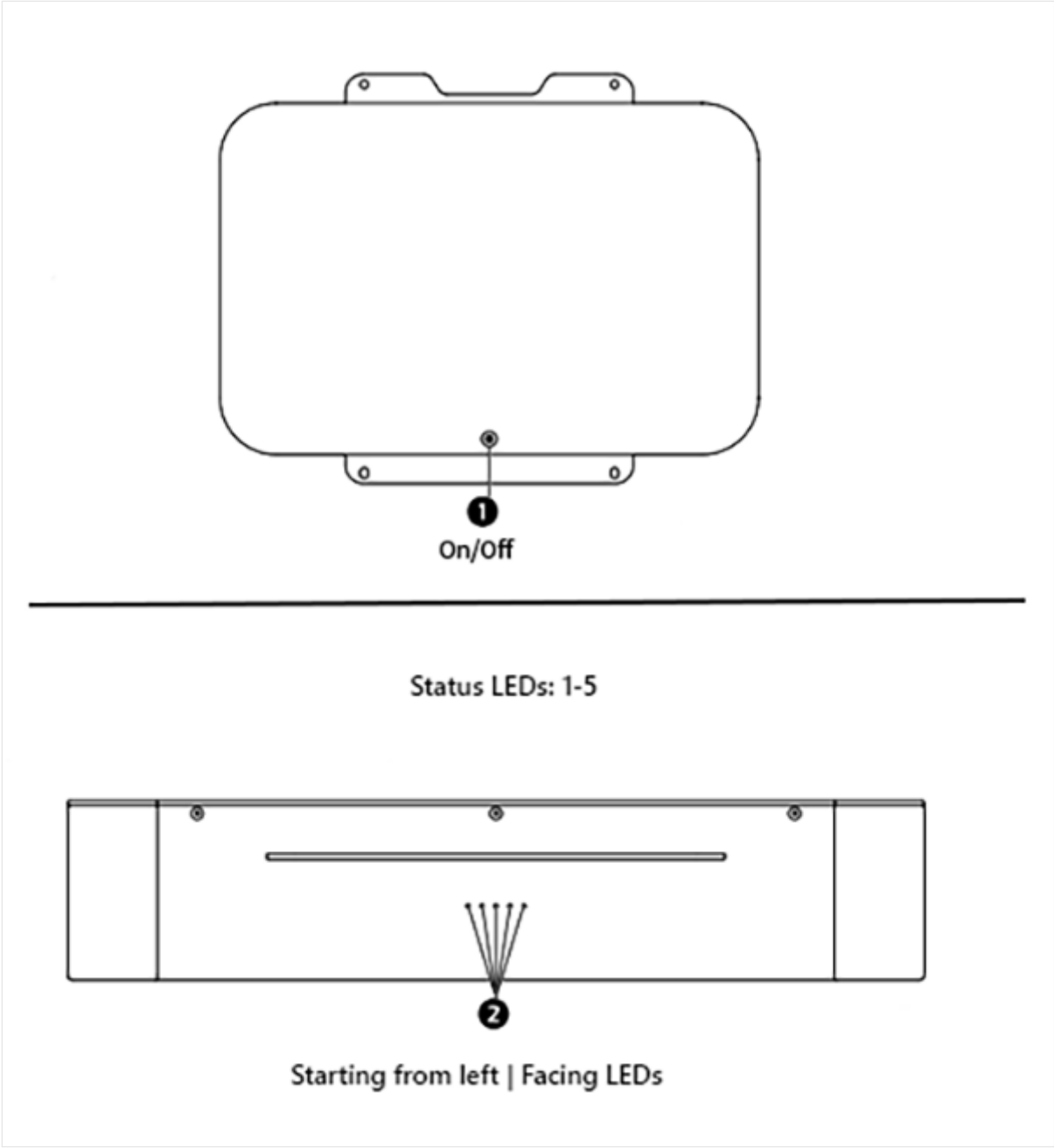


Figure 3. On/off button and LEDs indicating power function

> **Tip**
>
> The power on/off button is located on the bottom of the unit under a green sticker

C. Try to bypass the APC Charge Mobile Battery and power the Surface Hub 2S directly via the **AC power cord** to the power source. Does the Surface Hub 2S power on independently?

Support requests

If your Surface Hub 2S does power on properly while bypassing the APC Charge Mobile Battery (step 3), contact the APC by Schneider Electric Customer Support Center **for**

battery support and include the following details:

- Model number of APC Charge Mobile Battery.
- Serial number of APC Charge Mobile Battery.
- Date of purchase.
- Results of Basic Troubleshooting steps outlined on the APC FAQs page.
- Results of the troubleshooting steps outlined on this page.

> **Tip**
>
> The model and serial numbers are located on the top panel of the APC Charge Mobile Battery.

Or if your Surface Hub doesn't power on despite bypassing the APC Charge Mobile Battery (step C), refer to Troubleshoot Surface Hub 2S power and contact Microsoft for support regarding Surface Hub 2S.

Learn more

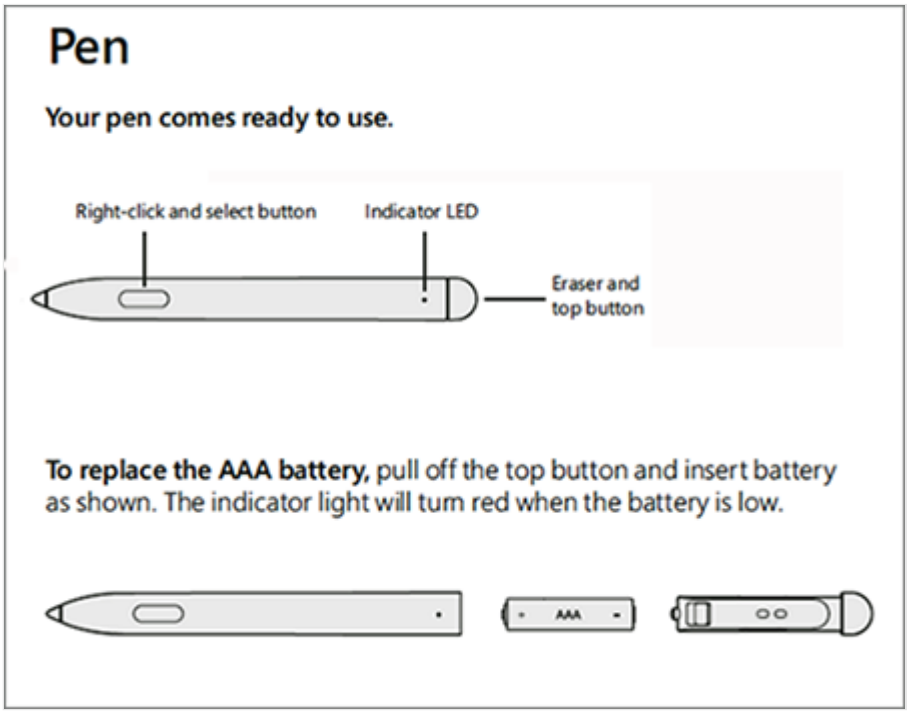
- APC Charge Mobile Power Supply User Manual.

Troubleshoot Surface Hub 2 pen

Article • 03/01/2023 • Applies to: Surface Hub 2S

If you encounter issues with your Surface Hub 2 pen, follow the troubleshooting steps on this page.

1. First, make sure your pen has a working battery. If the indicator light on the pen shows **solid white**, the pen is ready for use. If the indicator light shows **solid red** or no light, replace the battery on the pen. The Surface Hub 2S pen requires a single **AAA battery.**



2. If the pen isn't functioning as expected, pair it to Surface Hub 2S via Bluetooth to ensure it's running the latest firmware. Press and hold the Eraser and top button until the indicator light starts blinking. This enables the pen to be discoverable via Bluetooth.

> **Tip**
>
> If the indicator light does not start blinking (even with new a new battery), try reseating the eraser cap.

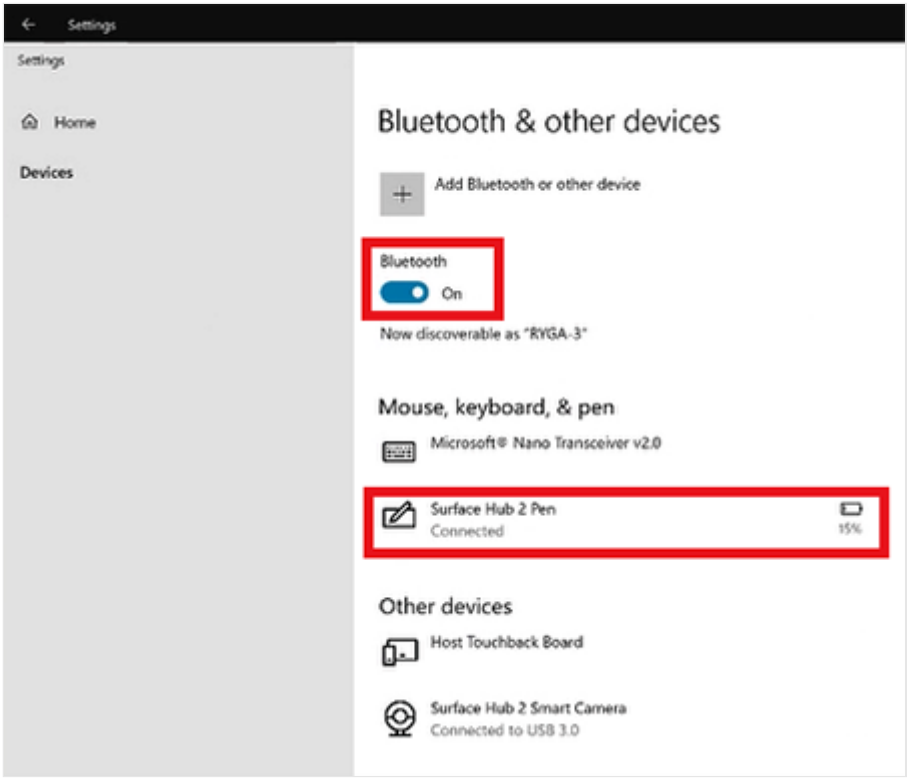
1. Navigate to **Settings** > **sign in as an administrator** and select **Devices (Bluetooth, printers, mouse).**

2. Ensure Bluetooth is turned **On.**

3. If the pen is already connected to the Surface Hub, you should see **Surface Hub 2 Pen** listed under **Mouse, keyboard, & pen.**

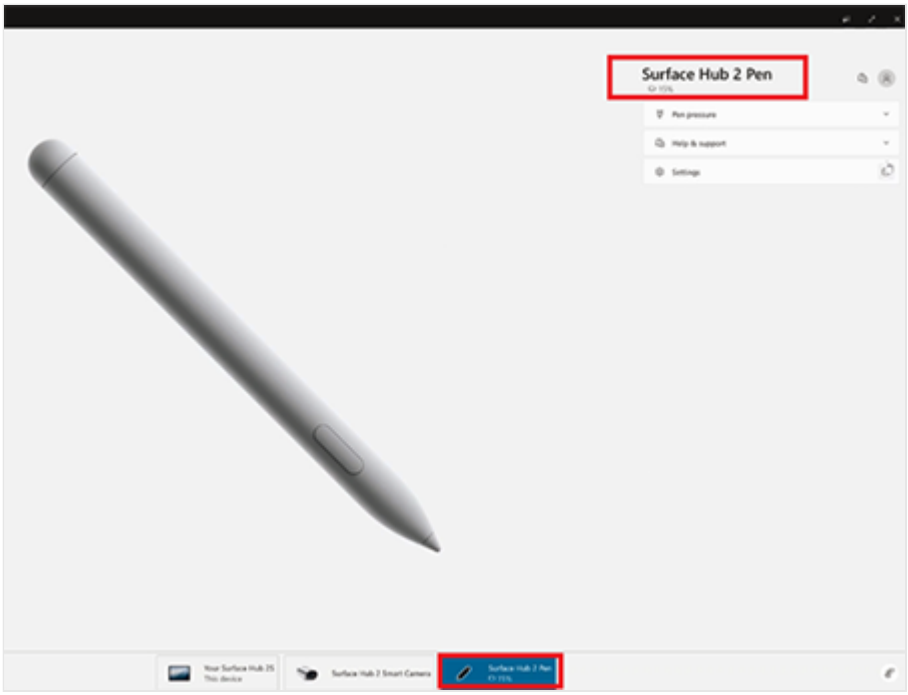
4. If you don't see the pen listed here, select the + button to **Add Bluetooth or other device.**

5. Once you see the **Surface Hub 2 Pen** listed in the results, you can add the pen from here.

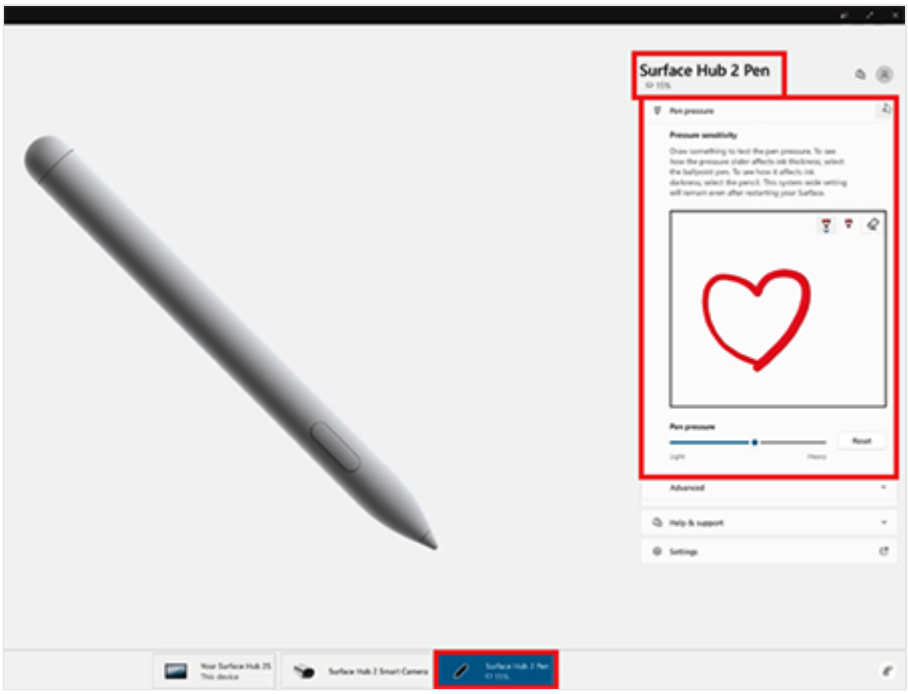


6. To see the battery level for your pen, navigate to **All Apps** > **Surface** > select the **Surface Hub 2S Pen.**

7. Ensure your Surface Hub 2S pen firmware is up to date, as outlined here: Update pen firmware on Surface Hub 2S



8. You can also adjust the pressure settings for your pen in the Surface app under the **Pen pressure** drop-down:



Support requests

If you're still unable to use the pen with your Surface Hub 2S, you'll need to acquire a replacement pen. The first step is to identify the warranty status of your device using the serial number of your Surface Hub 2S.

> **Tip**

You can find the serial number on the outside of the packaging, on the display by the power cord, or by using the Surface app.

If the warranty for your Surface Hub 2S is expired, you can order a replacement pen directly through the Microsoft Store.

If your device is still covered under warranty, please create a support request and include the following items as it will help speed up the process:

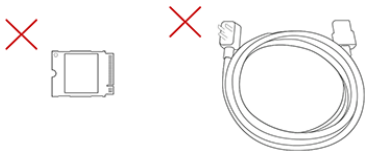
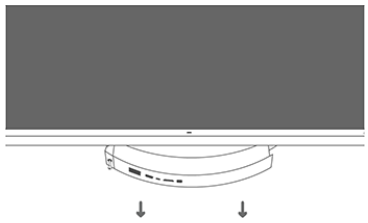
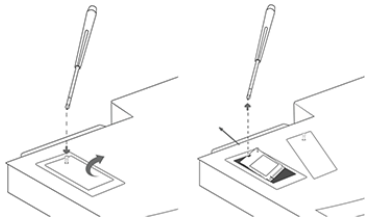
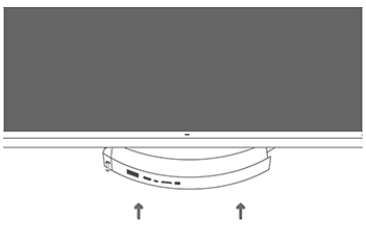
- Results of troubleshooting steps on this page.
- Shipping address and recipient contact information.
- Serial number of the **Surface Hub 2S** (not the pen itself).

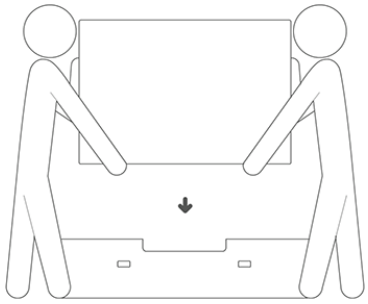
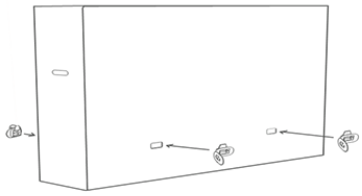
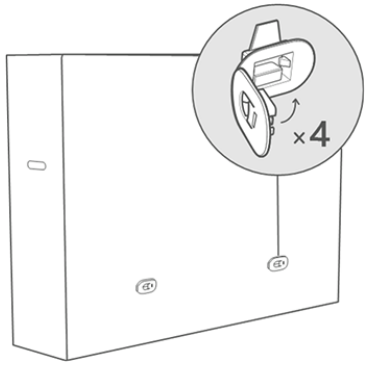
How to pack and ship Surface Hub 2S

Article • 02/22/2023

This article explains how to pack Surface Hub 2S for shipment or service.

> **ⓘ Important**
>
> When packing your device for shipment, make sure that you use the original packaging that came with Surface Hub 2S.

Step	Task	Illustration
1.	Remove the pen and the camera. Don't pack them with the unit.	
2.	Remove the drive and the power cable. Don't pack them with the unit. Don't pack the Setup guide with the unit.	
3.	Unplug all cables, slide the cover sideways, and unscrew the locking screw of the compute cartridge.	
4.	Slide the compute cartridge out of the unit.	
5.	You'll need the compute cartridge and a screwdriver.	
6.	Remove the cover screw and the cover from the compute cartridge, and then remove the solid state drive (SSD).	
7.	Replace the cover and slide the compute cartridge back into the unit.	

Step	Task	Illustration
8.	Refasten the locking screw and slide the cover into place.	
9.	Remove any base or mounting hardware. Using two people, place the unit in the base of the shipping container.	
10.	Replace the cover of the shipping container, and insert the four clips.	
11.	Close the four clips.	

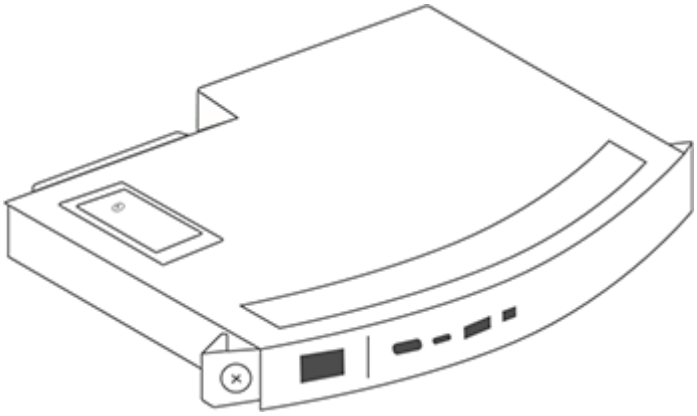
Learn more

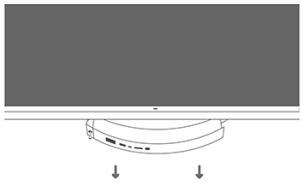
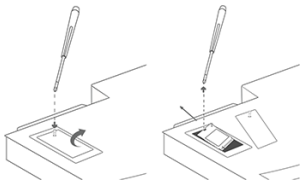
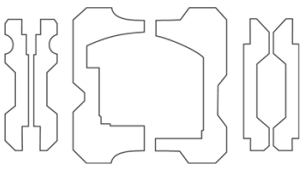
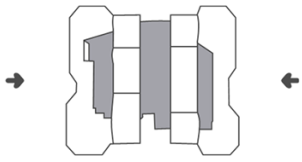
- Remove, replace & install Surface Hub 2S compute cartridge
- Remove or replace Surface Hub 2S Camera

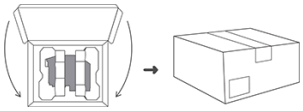
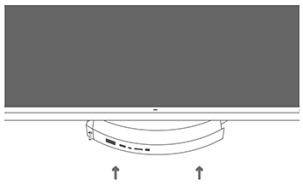
Replace & install compute cartridge on Surface Hub 2S

Article • 02/22/2023 • Applies to: Surface Hub 2S

This article explains how to remove the Surface Hub 2S compute cartridge, pack it for shipment, and install a new compute cartridge.



Step	Task	Illustration
1.	Unplug all cables, slide the cover sideways, and unscrew the locking screw of the compute cartridge.	
2.	Slide the compute cartridge out of the unit.	
3.	You'll need the compute cartridge and a screwdriver.	
4.	Remove the cover screw and the cover from the compute cartridge, and then remove the solid state drive (SSD). When finished, replace the cover.	
5.	You'll need the original packaging for your replacement compute cartridge.	
6.	Place the old compute cartridge in the packaging.	

Step	Task	Illustration
7.	Place the old compute cartridge and its packaging into the box that was used for the replacement compute cartridge. Reseal the box.	
8.	Slide the replacement compute cartridge into the unit.	
9.	Fasten the locking screw and slide the cover into place	

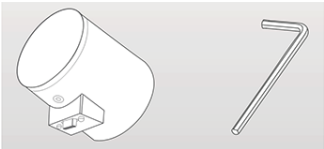
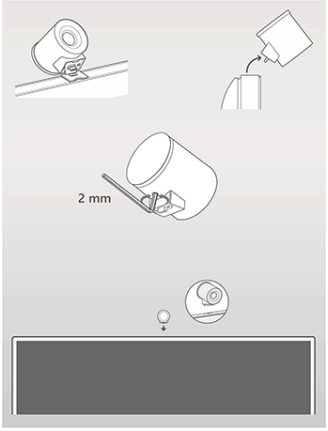
Learn more

- How to pack and ship your Surface Hub 2S for service
- Remove or replace Surface Hub 2S Camera

Replace & install camera on Surface Hub 2S

Article • 02/22/2023 • Applies to: Surface Hub 2S

This article explains how to remove the Surface Hub 2S camera and install a replacement camera or the Surface Hub 2 Smart Camera.

Step	Task	Illustration
1.	You'll need the new camera and the 2-millimeter allen wrench.	
2.	Unplug the old camera from the unit. If needed, use the allen wrench to adjust the new camera. Plug the new camera into the unit.	

Learn more

- Install and Manage Surface Hub 2 Smart Camera
- How to pack and ship your Surface Hub 2S for service
- Remove, replace & install Surface Hub 2S compute cartridge

Surface Hub Third-Party Stand Policy and Waiver

Article • 05/11/2023

This article provides Surface Hub Third-Party Stand Policy and Waiver for each country or region. To download the document, select the country or region where you purchased your Surface Hub.

To find other warranty terms in your country or region, go to Warranties, extended service plans, and Terms & Conditions for your device.

> **Note**
>
> To read the documents on this page, you must use a PDF viewer, PDF-enabled browser, or view through a device with PDF features enabled.

- Australia - English
- Belgique - Français
- België - Nederlands
- Canada - English
- Canada - Français
- Danmark - Dansk
- Deutschland - Deutsch
- España - Español
- France - Français
- Ireland - English
- Italia - Italiano
- Luxembourg - Deutsch
- Luxembourg - Français
- Malaysia - English
- Nederland - Nederlands
- New Zealand - English
- Norge - Bokmål
- Portugal - Português
- Qatar - English
- Schweiz - Deutsch
- Singapore - English
- Suisse - Français
- Suomi - Suomi

- Sverige - Svenska
- United Arab Emirates - English
- United Kingdom - English
- United States - English
- Österreich - Deutsch

Surface Hub (v1) 55" tech specs

Article • 02/16/2023 • Applies to: Surface Hub

Feature	Description
Pricing	Starting at $8,999
Size	31.75” x 59.62” x 3.38” (806.4mm x 1514.3mm x 85.8mm)
Storage/RAM	SSD 128GB with 8GB RAM
Processor	4th Generation Intel® Core™ i5
Graphics	Intel® HD 4600
Ports	**Internal PC** • (1) USB 3.0 (bottom) + (1) USB 3.0 (side access) • (2) USB 2.0 • Ethernet 1000 Base-T • DisplayPort • Video Output • 3.5mm Stereo Out • RJ11 Connector for system-level control **Alternate PC** • (2) USB 2.0 type B output • Connection for Camera, Sensors, Microphone, Speakers • (1) DisplayPort Video Input **Guest PC** • DisplayPort Video Input • HDMI Video Input • VGA Video Input • 3.5mm Stereo Input • (1) USB 2.0 type B Touchback™ Output
Sensors	(2) Passive Infrared Presence Sensors, Ambient Light Sensors
Speakers	(2) Front-facing stereo speakers
Microphone	High-Performance, 4-Element Array
Camera	(2) Wide angle HD cameras 1080p @ 30fps
Pen	(2) Powered, active, subpixel accuracy
Physical side buttons	Power, Input Select, Volume, Brightness
Software	Windows 10 + Office (Word, PowerPoint, Excel)

Feature	Description
What's in the box	• Surface Hub 55" • (2) Surface Hub Pens • Power Cable • Setup Guide • Start Guide • Safety and Warranty documents • Wireless All-in-One Keyboard
Mounting features	4X VESA standard, 400mm x 400mm plus 1150mm x 400mm pattern, 8X M6 X 1.0 threaded mounting locations
Display height from floor	Recommended height of 55 inches (139.7 cm) to center of screen
Product weight	Approx. 105 lb. (47.6 kg) without accessories
Product shipping weight	Approx. 150 lb. (68 kg)
Product dimensions HxWxD	31.63 x 59.62 x 3.2 inches (80.34 x 151.44 x 8.14 cm)
Product shipping dimensions HxWxD	43 x 65 x 20 inches (109 x 165 x 51 cm)
Product thickness	Touch surface to mounting surface: ≤ 2.4 inches (6 cm)
Orientation	Landscape only. Display cannot be used in a portrait orientation.
BTU	1706 BTU/h
Image resolution	1920 x 1080
Frame rate	120Hz
EDID preferred timing, replacement PC	1920 x 1080, 120Hz vertical refresh
EDID preferred timing, wired connect	1920 x 1080, 60Hz vertical refresh
Input voltage	(50/60Hz) 110/230v nominal, 90-265v max
Input power, operating	500W max
Input power, standby	5W nominal

Note

Surface Hub can be used continuously for a maximum of 18 hours a day. To optimize for efficiency, Surface Hub uses smart sensors to turn off the LED screen when presence is no longer detected, which means there is no need to power it down at the end of the day. If the unit is installed in a 24-hour workplace environment, the sensors can be disabled to comply with the 18 hour per day maximum use recommendation. Note that prolonged display of a video signal may cause burned-in or image retention to occur on the screen. To learn more about managing power settings, see:

- Local management Surface Hub settings
- SurfaceHub CSP - Windows Client Management

Replacement PC connections

Connector and location	Label	Description
Switch, bottom I/O		Switches the function between using internal PC or external PC.
Display port, bottom I/O		Provides input for replacement PC.
USB type B, bottom I/O		Provides USB connection for replacement PC to internal peripherals.
USB type B, bottom I/O		Provides USB connection for integrated hub.

Wired connect connections

Connector and location	Label	Description
Display port, bottom I/O		Provides input for wired connect PC.
HDMI, bottom I/O		Provides HDMI input for wired connect PC.
VGA, bottom I/O		Provides VGA input for wired connect PC.
3.5mm, bottom I/O		Provides analog audio input.

Connector and location	Label	Description
USB type B, bottom I/O		Provides USB connection for video ingest touchback.

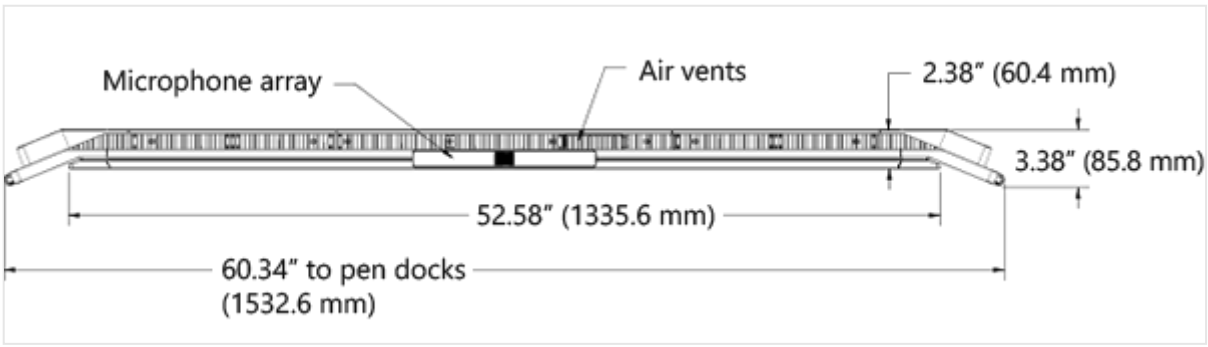
Additional connections

Connector and location	Label	Description
USB type A, side I/O		Provides 1 USB 3.0 connection for USB devices. Wake-on USB capable.
USB type A, bottom I/O with blue insulator		Provides USB 3.0 connection.
3.5mm, bottom I/O		Provides analog audio out.
Display port, bottom I/O		Provides mirrored video out function to another display.
IEC/EN60320-C13 receptacle with hard switch		Provides AC input and compliance with EU power requirements.
RJ45, bottom I/O		Connects to Ethernet.
RJ11, bottom I/O		Connects to room control systems.

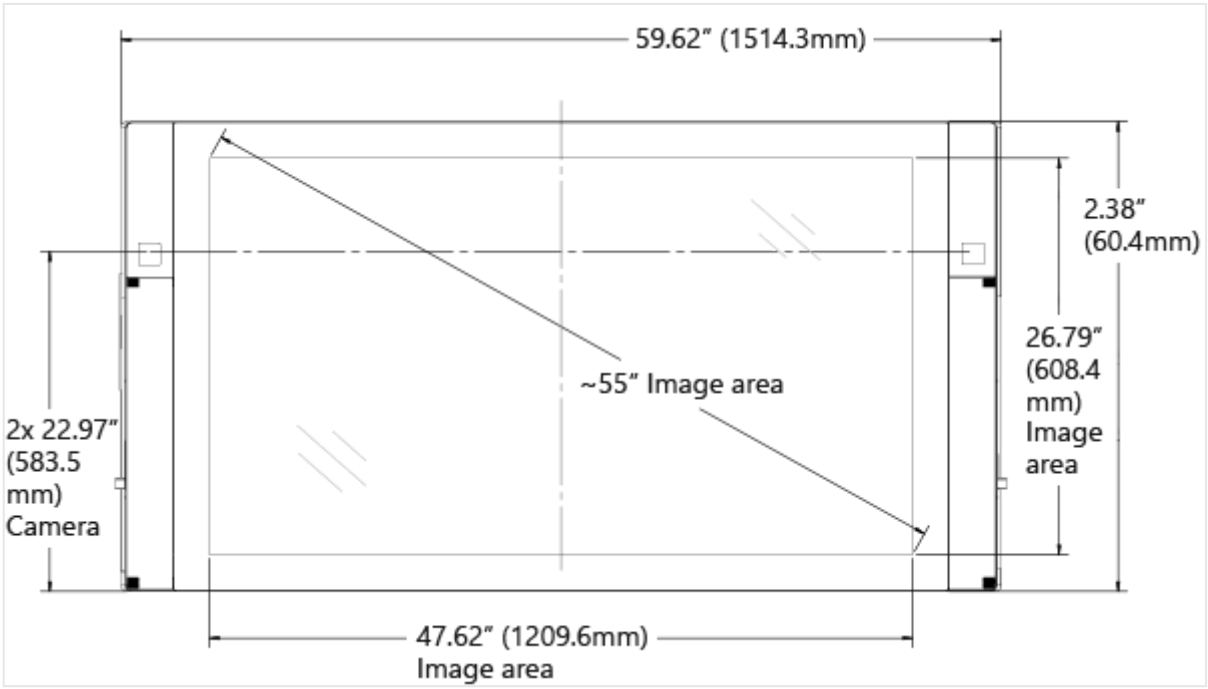
> **Note**
>
> Surface Hub can be used continuously for a maximum of 18 hours a day. To optimize for efficiency, Surface Hub uses smart sensors to turn off the LED screen when presence is no longer detected, which means there is no need to power it down at the end of the day. If the unit is installed in a 24-hour workplace environment, the sensors can be disabled to comply with the 18 hour per day maximum use recommendation. Note that prolonged display of a video signal may cause burned-in or image retention to occur on the screen. To learn more about managing power settings, see:
>
> - Local management Surface Hub settings
> - SurfaceHub CSP - Windows Client Management

Diagrams of ports and clearances

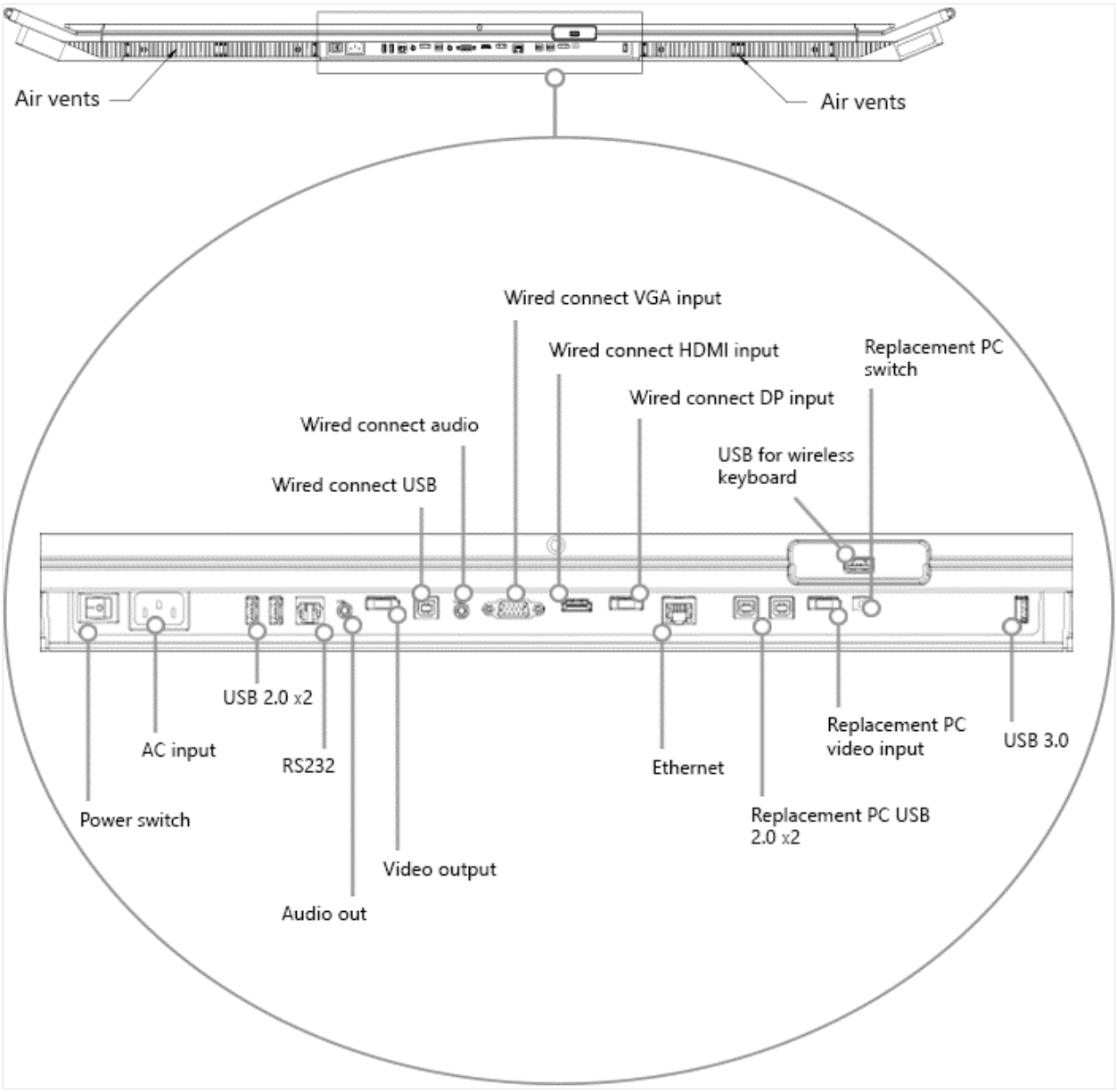
Top view of 55" Surface Hub



Front view of 55" Surface Hub

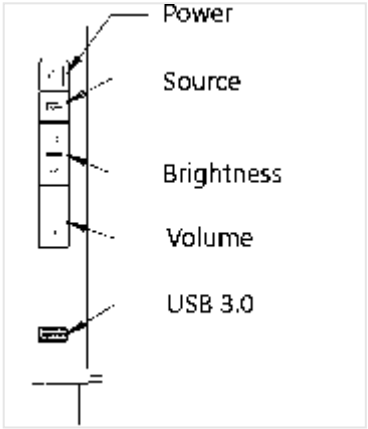


Bottom view of 55" Surface Hub

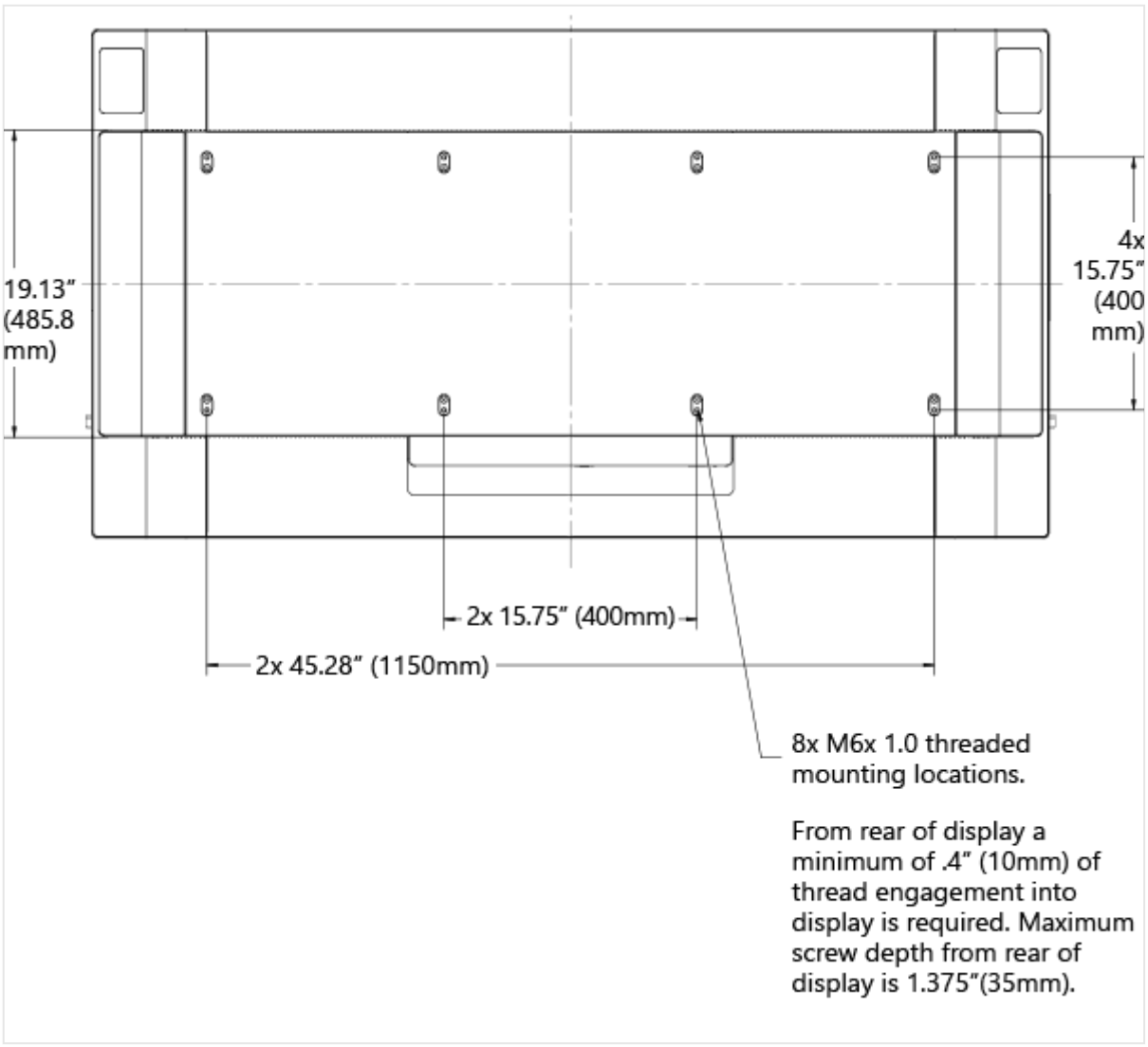


Replacement PC ports on 55" Surface Hub

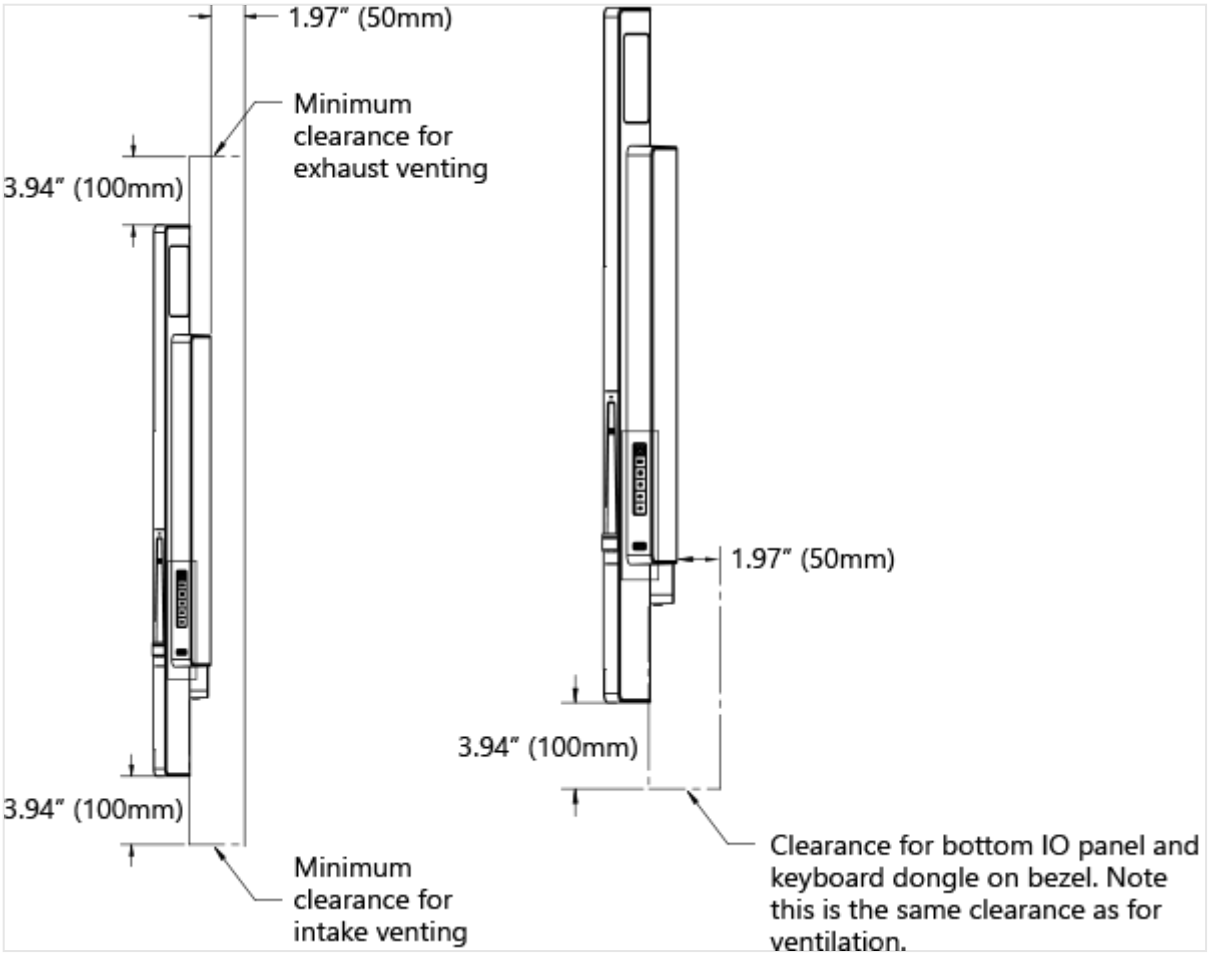
Keypad on right side of 55" Surface Hub



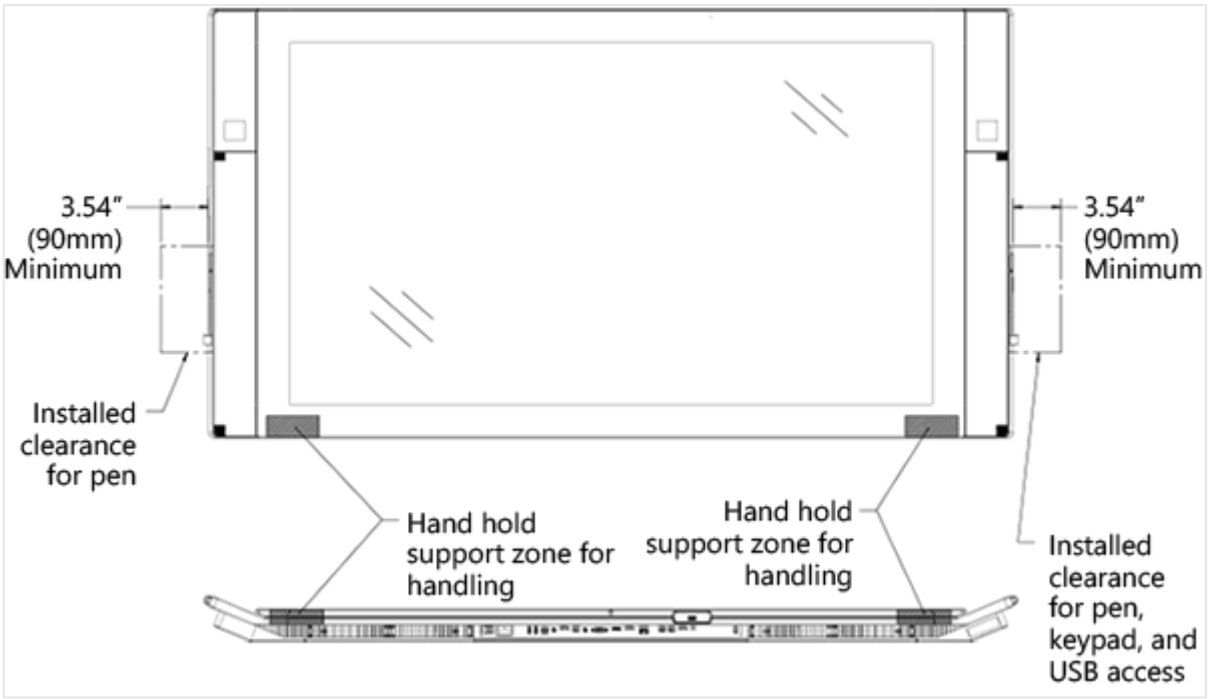
Rear view of 55" Surface Hub



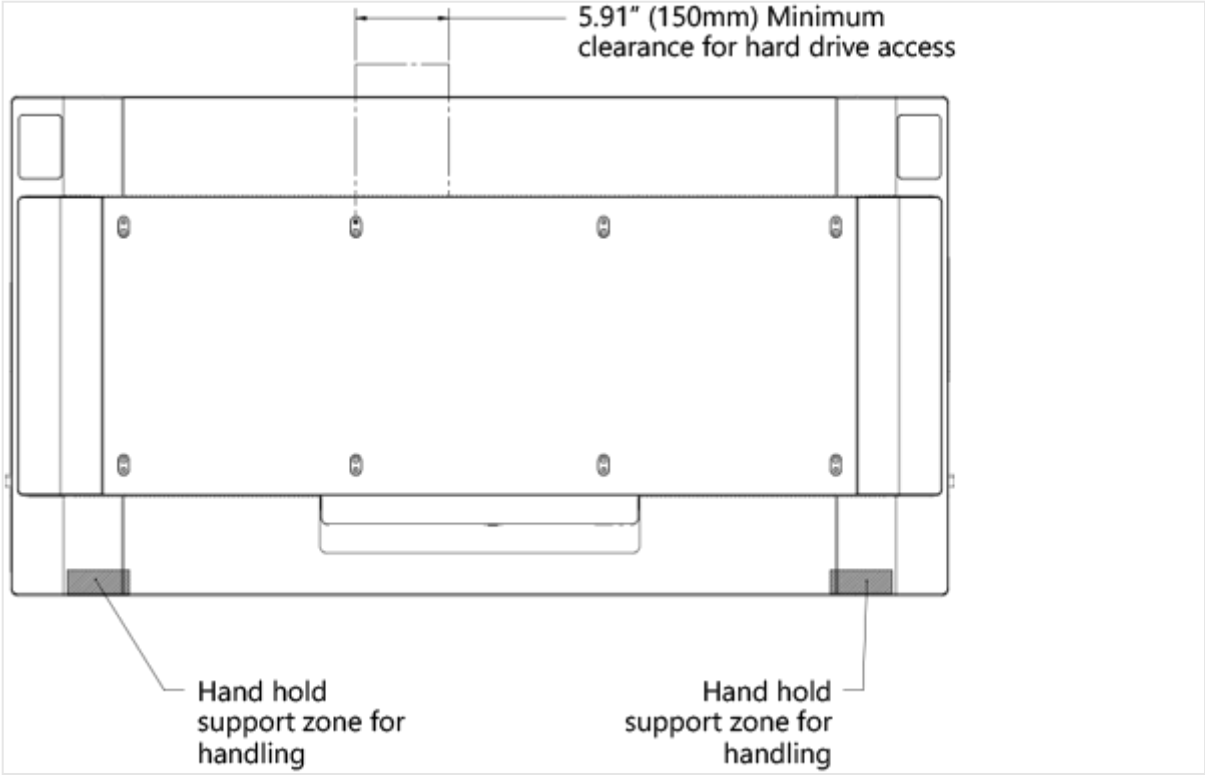
Clearances for 55" Surface Hub



Front and bottom handholds and clearances for 55" Surface Hub



Rear handholds and clearances for 55" Surface Hub


5.91” (150mm) Minimum
clearance for hard drive access
Hand hold
support zone for
handling
Hand hold
support zone for
handling

Surface Hub (v1) 84" tech specs

Article • 02/16/2023 • Applies to: Surface Hub

Feature	Description
Pricing	Starting at $21,999
Size	46.12” x 86.7” x 4.15” (1171.5mm x 2202.9mm x 105.4mm)
Storage/RAM	SSD 128GB with 8GB RAM
Processor	4th Generation Intel® Core™ i7
Graphics	NVIDIA Quadro K2200
Ports	**Internal PC** • (1) USB 3.0 (bottom) + (1) USB 3.0 (side access) • (4) USB 2.0 • Ethernet 1000 Base-T • DisplayPort Video Output • 3.5mm Stereo Out • RJ11 Connector for system-level control **Alternate PC** • (2) USB 2.0 type B output • connection for Camera, Sensors, Microphone, Speakers • (2) DisplayPort Video Input **Guest PC** • DisplayPort Video Input • HDMI Video Input • VGA Video Input • 3.5mm Stereo Input • (1) USB 2.0 type B Touchback™ Output
Sensors	(2) Passive Infrared Presence Sensors, Ambient Light Sensors
Speakers	(2) Front-facing stereo speakers
Microphone	High-Performance, 4-Element Array
Camera	(2) Wide angle HD cameras 1080p @ 30fps
Pen	(2) Powered, active, subpixel accuracy
Physical side buttons	Power, Input Select, Volume, Brightness
Software	Windows 10 + Office (Word, PowerPoint, Excel)

Feature	Description
What's in the box	• Surface Hub 84" • (2) Surface Hub Pens • Power Cable • Setup Guide • Safety and Warranty documents • Wireless All-in-One Keyboard
Mounting features	4X VESA standard, 1200mm x 600mm pattern, 8X M8 X 1.25 threaded mounting locations
Display height from floor	Recommended height of 54 inches (139.7 cm) to center of screen
Product weight	Approx. 280 lb. (127 kg.)
Product shipping weight	Approx. 580 lb. (263 kg.)
Product dimensions HxWxD	46 x 86.9 x 4.1 inches (116.8 x 220.6 x 10.4 cm)
Product shipping dimensions HxWxD	66.14 x 88.19 x 24.4 inches (168 x 224 x 62 cm)
Product thickness	Touch surface to mounting surface: ≤ 3.1 inches (7.8 cm)
Orientation	Landscape only. Display cannot be used in a portrait orientation.
BTU	3070.8 BTU/h
Image resolution	3840 x 2160
Frame rate	120Hz
Contrast Ratio	1400:1
EDID preferred timing, replacement PC	3840 x 2140, 120Hz vertical refresh
EDID preferred timing, wired connect	1920 x 1080, 60Hz vertical refresh
Input voltage	110/230v nominal, 90-265v max
Input power, operating	900W max
Input power, standby	5W nominal, 1-10W max

ⓘ Note

Surface Hub can be used continuously for a maximum of 18 hours a day. To optimize for efficiency, Surface Hub uses smart sensors to turn off the LED screen

when presence is no longer detected, which means there is no need to power it down at the end of the day. If the unit is installed in a 24-hour workplace environment, the sensors can be disabled to comply with the 18 hour per day maximum use recommendation. Note that prolonged display of a video signal may cause burned-in or image retention to occur on the screen. To learn more about managing power settings, see:

- Local management Surface Hub settings
- SurfaceHub CSP - Windows Client Management

Replacement PC connections

Connector and location	Label	Description
Switch, bottom I/O		Switches the function between using internal PC or external PC.
Display port, bottom I/O		Provides input for replacement PC.
Display port, bottom I/O		Provides second input for replacement PC.
USB type B, bottom I/O		Provides USB connection for replacement PC to internal peripherals.
USB type B, bottom I/O		Provides USB connection for integrated hub.

Wired connect connections

Connector and location	Label	Description
Display port, bottom I/O		Provides input for wired connect PC.
HDMI, bottom I/O		Provides HDMI input for wired connect PC.
VGA, bottom I/O		Provides VGA input for wired connect PC.
3.5mm, bottom I/O		Provides analog audio input.

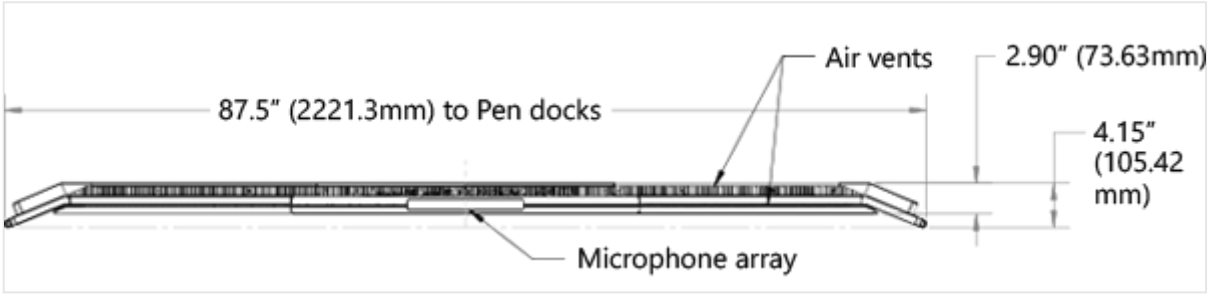
Connector and location	Label	Description
USB type B, bottom I/O		Provides USB connection for video ingest touchback.

Additional connections

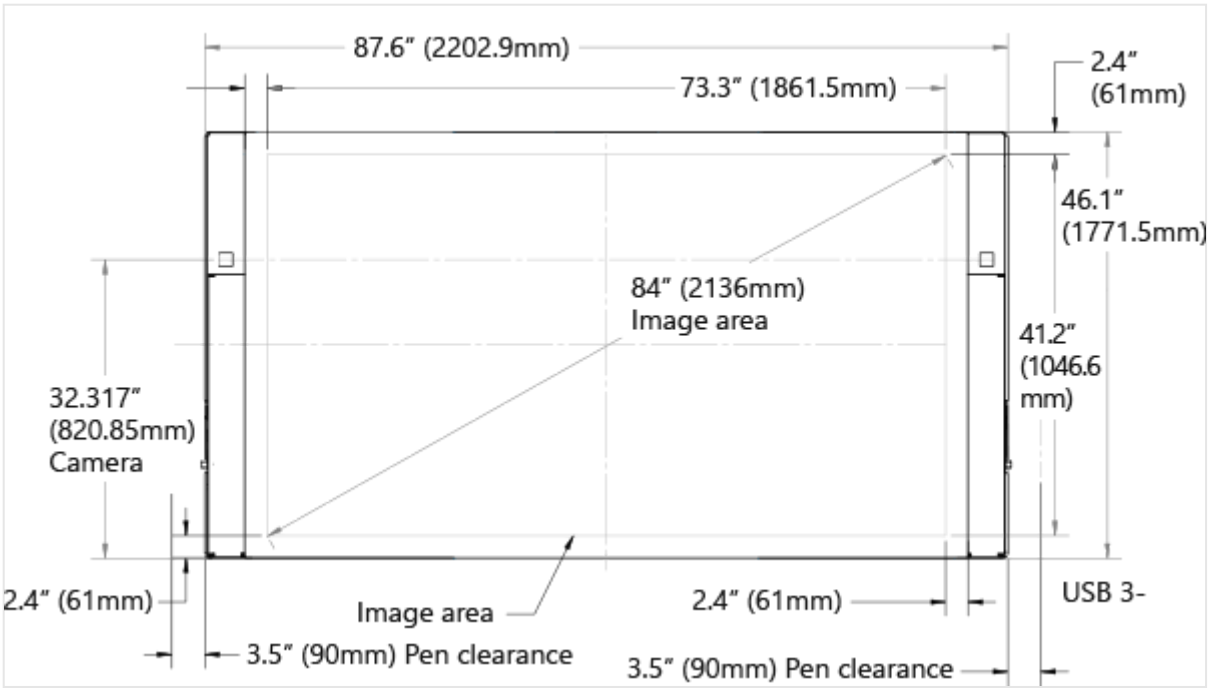
Connector and location	Label	Description
USB type A, side I/O		Provides 1 USB 3.0 connection for USB devices. Wake-on USB capable.
USB type A, bottom I/O with blue insulator		Provides USB 3.0 connection.
3.5mm, bottom I/O		Provides analog audio out.
Display port, bottom I/O		Provides mirrored video out function to another display.
IEC/EN60320-C13 receptacle with hard switch		Provides AC input and compliance with EU power requirements.
RJ45, bottom I/O		Connects to Ethernet.
RJ11, bottom I/O		Connects to room control systems.

Diagrams of ports and clearances

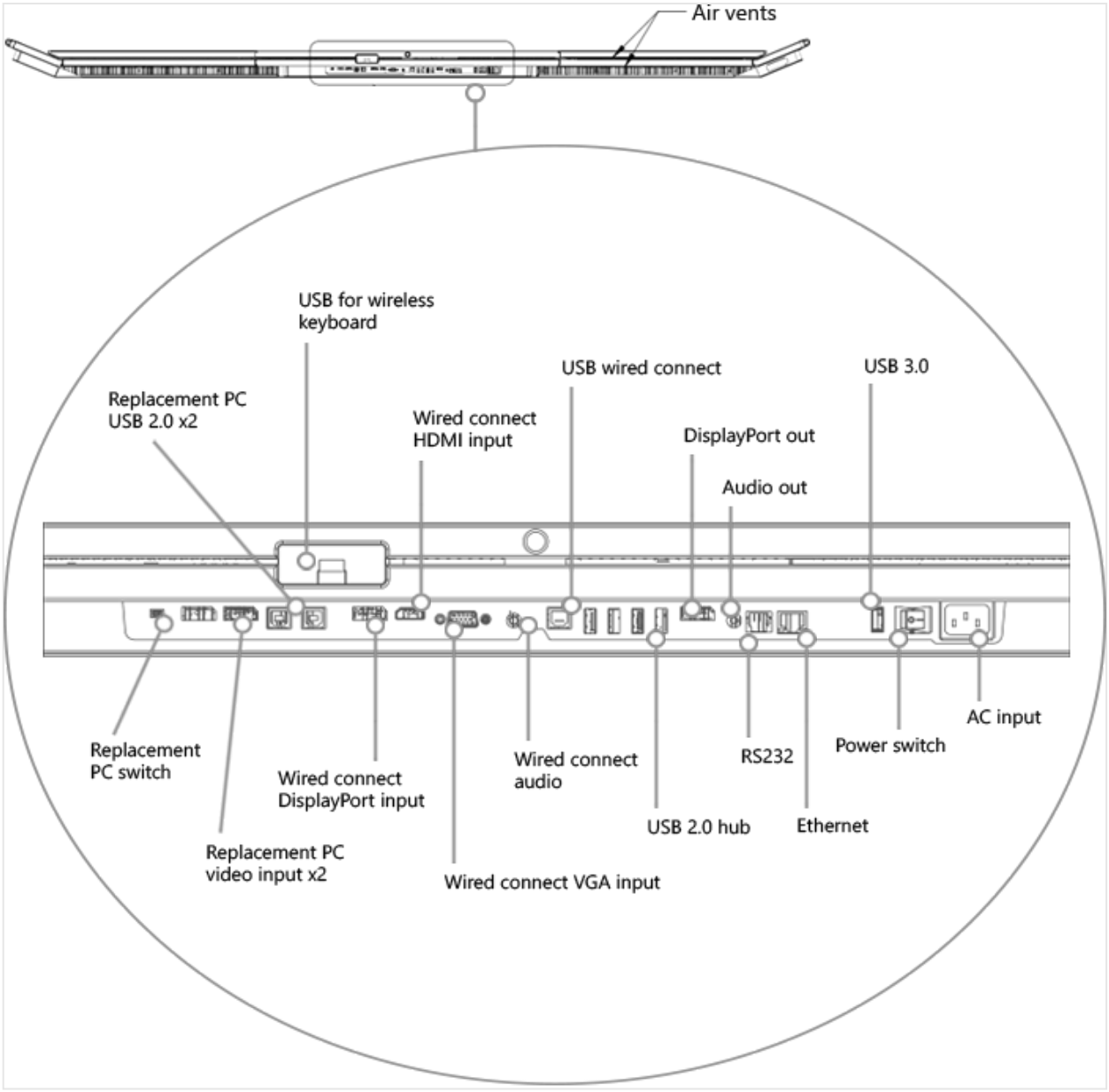
Top view of 84" Surface Hub



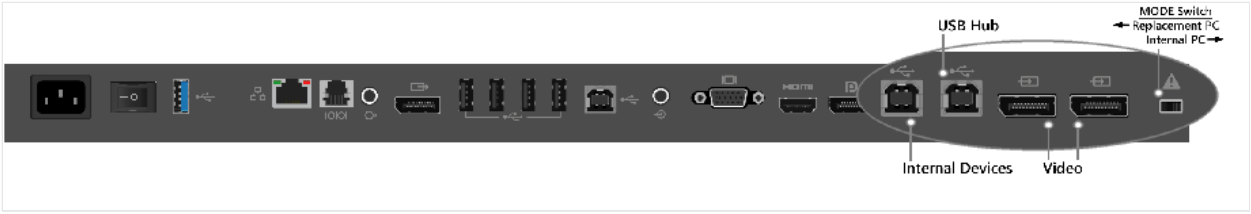
Front view of 84" Surface Hub



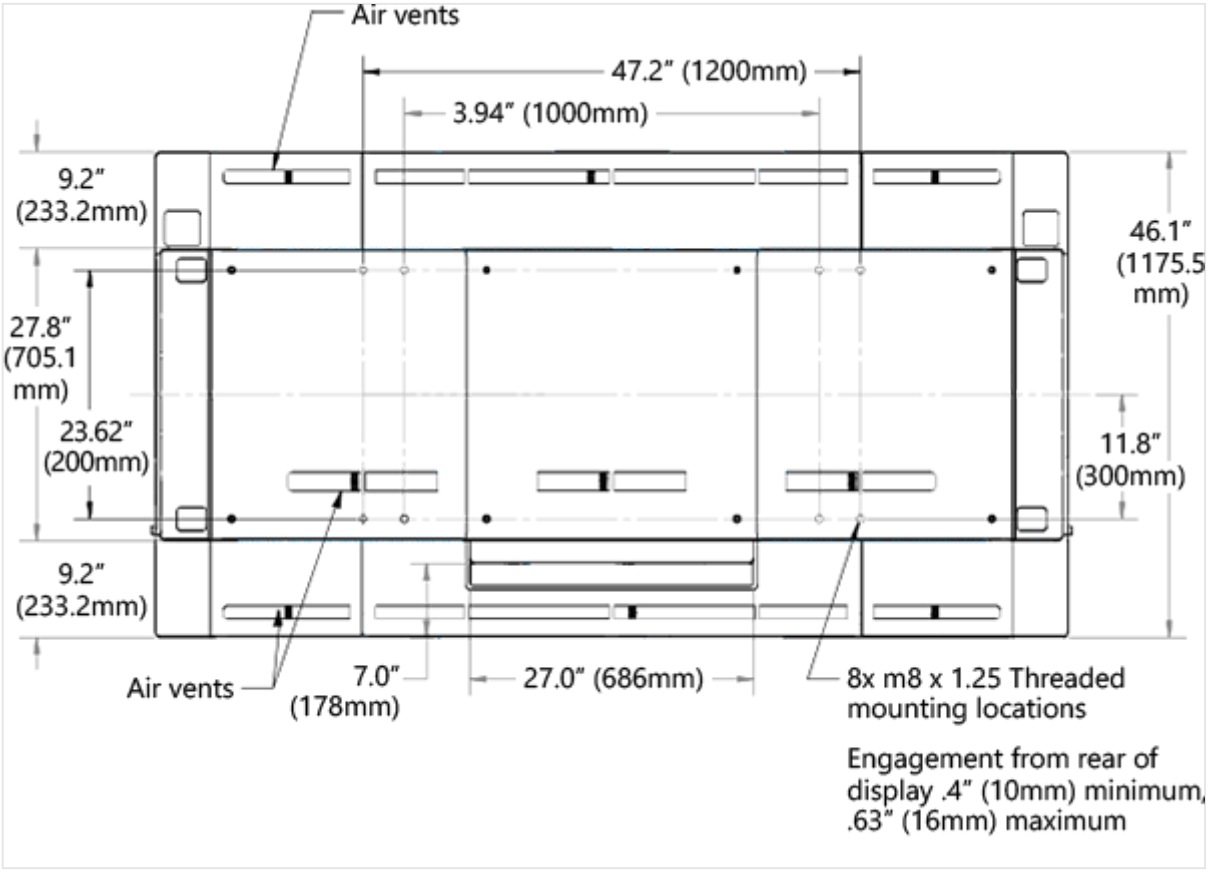
Bottom view of 84" Surface Hub



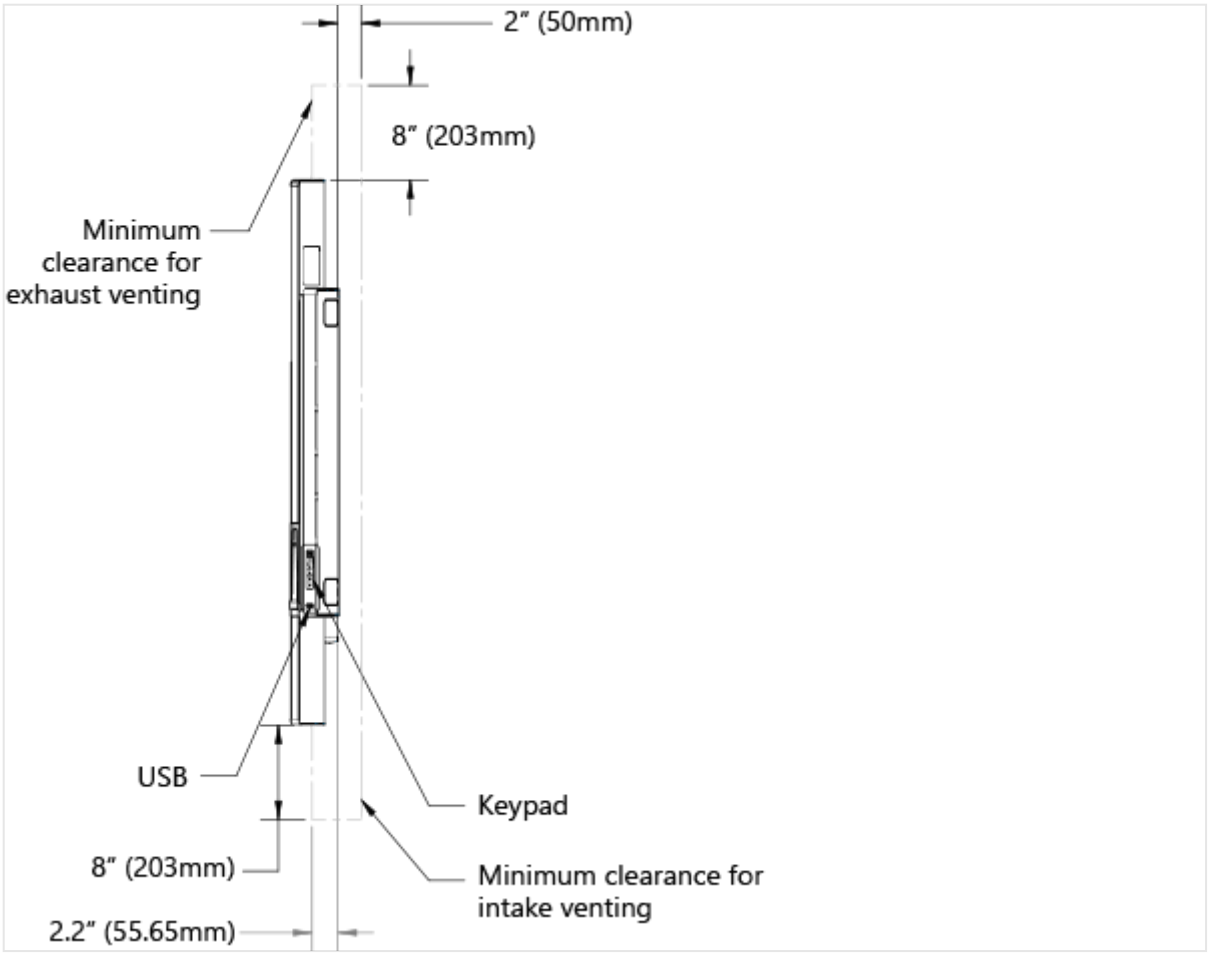
Replacement PC ports on 84" Surface Hub



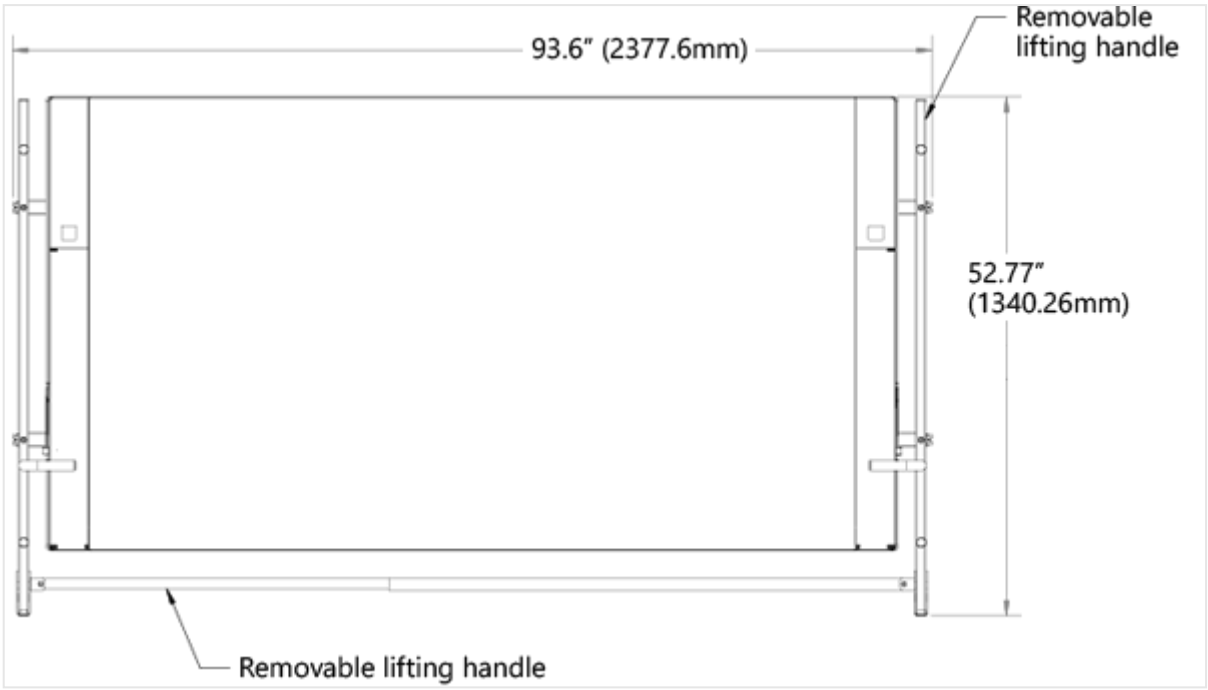
Rear view of 84" Surface Hub



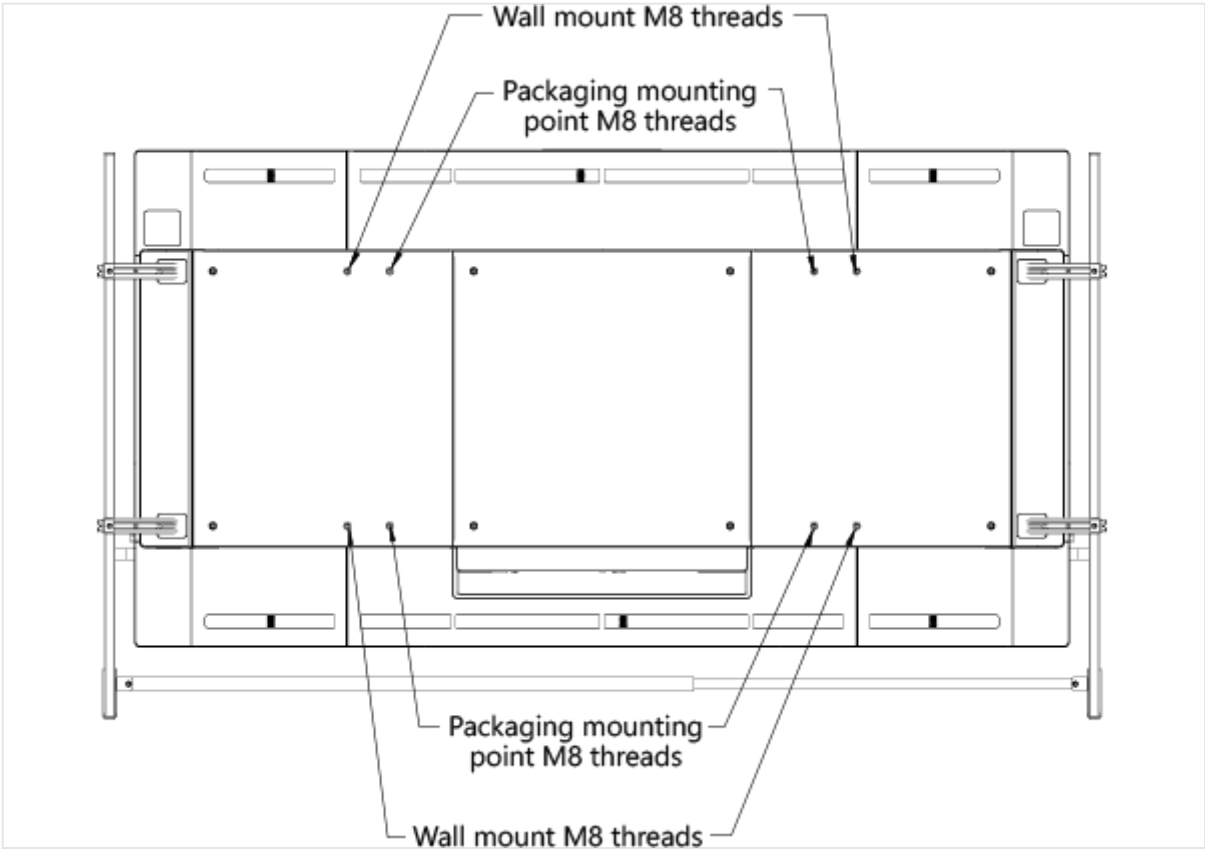
Clearances for 84" Surface Hub



Removable lifting handles on 84" Surface Hub

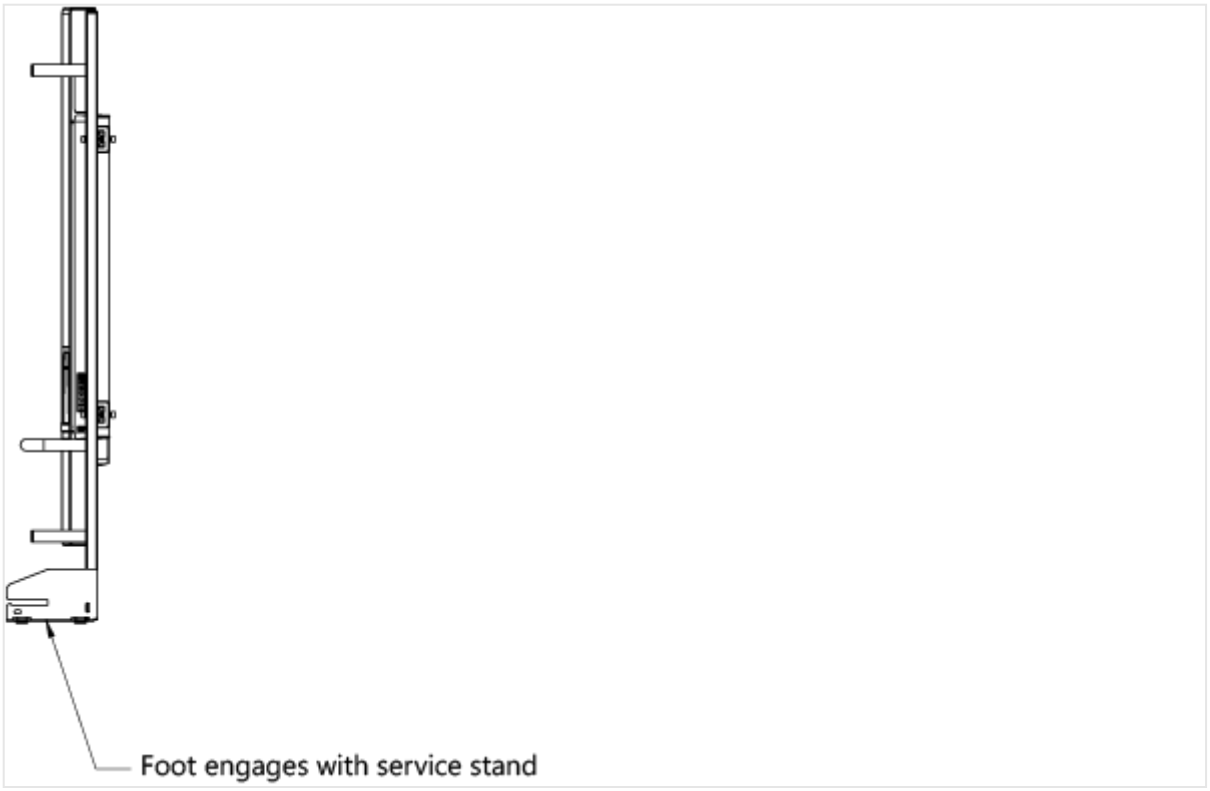


Wall mount threads on back of 84" Surface Hub



Lifting handles in top view of 84" Surface Hub

Side view of 84" Surface Hub


Foot engages with service stand

Surface Hub Site Readiness Guide

Article • 02/16/2023

Use this Site Readiness Guide to help plan your Surface Hub installation.

Site readiness planning

The room needs to be large enough to provide good viewing angles, but small enough for the microphones to pick up clear signals from the people in the room. Most rooms that are about 22 feet (seven meters) long will provide a good meeting experience. In the conference area, mount Surface Hub where:

- Everyone in the room can see it.
- People can reach all four edges of the touchscreen.
- The screen is not in direct sunlight, which could affect viewing or damage the screen.
- Ventilation openings are not blocked.
- Microphones are not affected by noise sources, such as fans or vents. You can find more details in the Surface Hub (v1) 55" tech specs or Surface Hub (v1) 84" tech specs sections.

Hardware considerations

Surface Hub arrives with:

- Two Microsoft Surface Hub pens
- A Microsoft wireless keyboard, customized for Surface Hub
- A 9-foot NEMA 5-15P (US Standard) to C13 power cable

You'll need to provide:

- Cat-5e or Cat-6 network cables
- Display cables (optional)
- Audio cable (optional)
- Type A to B USB cable (optional)

For details about cable ports, see the Surface Hub (v1) 55" tech specs or Surface Hub (v1) 84" tech specs sections. For details about cables, see Wired Connect.

Microsoft Surface Hub has an internal PC and does not require an external computer system.

For power recommendations, see Surface Hub (v1) 55" tech specs or Surface Hub (v1) 84" tech specs.

Data and other connections

To use Surface Hub, you need an active Ethernet port and a standard power outlet. In addition, you may want to:

- Equip the conference table for Wired Connect.
- Expand the wall outlet configuration to include:
  - Additional AC outlets
  - Ethernet ports
  - Audio ports
  - Video ports (DisplayPort, HDMI, VGA, etc.)

When Surface Hub arrives

Surface Hub is large and heavy, so let Receiving know when it will arrive and what they should do to handle it safely. For details on the packing weights and other specifications, see Surface Hub (v1) 55" tech specs or Surface Hub (v1) 84" tech specs.

Consider the following:

- Wait to unpack Surface Hub from the shipping container until you've moved it to the conference area where you plan to install it.
- Make sure your loading dock can accept a shipment on a pallet and hold it securely until it can be installed.
- Check for local labor union rules that would require you to use union labor to unload or move Surface Hub.
- Do not leave Surface Hub in a hot or humid environment. As with any computer-based or display equipment, heat and humidity can damage Surface Hub. The recommended storage temperatures are 32°F to 95°F with a relative humidity of less than 70 percent.

Moving Surface Hub

Before you move Surface Hub, make sure that all the doorways, thresholds, hallways, and elevators are big enough to accommodate it. For information on the dimensions and weight of your Surface Hub in its shipping container, see Surface Hub (v1) 55" tech specs or Surface Hub (v1) 84" tech specs.

Unpacking Surface Hub

For unpacking information, refer to the unpacking guide included in the shipping container. You can open the unpacking instructions before you open the shipping container.

> **ⓘ Important**
>
> Retain and store all Surface Hub shipping materials—including the pallet, container, and screws—in case you need to ship Surface Hub to a new location or send it for repairs. For the 84" Surface Hub, retain the lifting handles.

Lifting Surface Hub

The 55" Surface Hub requires two people to safely lift and mount. The 84" Surface Hub requires four people to safely lift and mount. Those assisting must be able to lift 70 pounds to waist height. Review the unpacking and mounting guide for details on lifting Surface Hub.

Mounting and setup

There are three ways to mount your Surface Hub:

- **Wall mount**: Lets you permanently hang Surface Hub on a conference space wall.
- **Floor support mount**: Supports Surface Hub on the floor while it is permanently anchored to a conference space wall.
- **Rolling stand**: Supports Surface Hub and lets you move it to other conference locations.

For specifications on available mounts for the original Surface Hub, see the following:

- Surface Hub Mounts and Stands Datasheet
- Surface Hub Stand and Wall Mount Specifications
- Downloadable resources for Surface Hub readiness

The Connect experience

Connect lets people project their laptop, tablet, or phone to the Surface Hub screen. Connect allows wireless or wired connection types.

Wireless connect

Since wireless connect is based on Miracast, you don't need cables or additional setup planning to use it. Your users can load Miracast on most Miracast-enabled Windows devices. Then they can project their display from their computer or phone to the Surface Hub screen.

Wired connect

With wired connect, a cable transmits information from computers, tablets, or phones to Surface Hub. There are three video cable options, and they all use the same USB 2.0 cable. The cable bundle can include one or all of these connection options.

- DisplayPort (DisplayPort cable + USB 2.0 cable)
- HDMI (HDMI cable + USB 2.0 cable)
- VGA (VGA cable + 3.5mm audio cable + USB 2.0 cable)

For example, to provide audio, video, and touchback capability to all three video options, your Wired Connect cable bundle must include:

- A DisplayPort cable
- An HDMI cable
- A VGA cable
- A USB 2.0 cable
- A 3.5mm cable

When you create your wired connect cable bundles, check the Surface Hub (v1) 55" tech specs or Surface Hub (v1) 84" tech specs sections for specific technical and physical details and port locations for each type of Surface Hub. Make the cables long enough to reach from Surface Hub to where the presenter will sit or stand.

Physically install Microsoft Surface Hub

Article • 01/03/2023

The Microsoft Surface Hub Readiness Guide will help make sure that your site is ready for the installation. It includes planning information for both the 55" and 84" devices, as well as info on moving the Surface Hub from receiving to the installation location, mounting options, and a list of what's in the box.

You may also want to check out the Unpacking Guide. It will show you how to unpack the devices efficiently and safely. There are two guides, one for the 55" and one for the 84". A printed version of the Unpacking Guide is attached to the outside front of each unit's shipping crate.

- Download the 55" Unpacking Guide from the Microsoft Download Center.
- Download the 84" version from the Microsoft Download Center.

PowerShell for Surface Hub (v1)

Article • 01/03/2023 • Applies to: Surface Hub

> **Note**
>
> This page includes PowerShell scripts intended for the original Surface Hub (v1). For the latest account creation scripts for Surface Hub 2S, see **Create and test a device account**.

- PowerShell scripts for Surface Hub admins
  - Create an on-premises account
  - Create a device account using Office 365
  - Account verification script
  - Enable Skype for Business (EnableSfb.ps1)
- Useful cmdlets
  - Creating a Surface Hub-compatible Exchange ActiveSync policy
  - Allowing device IDs for ActiveSync
  - Auto-accepting and declining meeting requests
  - Accepting external meeting requests

> **Note**
>
> See also **Modern Auth and Unattended Scripts in Exchange Online PowerShell V2**

Prerequisites

To successfully execute these PowerShell scripts, you will need to install the following prerequisites:

- Microsoft Online Services Sign-in Assistant for IT Professionals RTW
- Microsoft Azure Active Directory Module for Windows PowerShell (64-bit version)
- Windows PowerShell Module for Skype for Business Online

PowerShell scripts for Surface Hub administrators

What do the scripts do?

- Create device accounts for setups using pure single-forest on-premises (Microsoft Exchange and Skype 2013 and later only) or online (Microsoft Office 365), that are configured correctly for your Surface Hub.
- Validate existing device accounts for any setup (on-premises or online) to make sure they're compatible with Surface Hub.
- Provide a base template for anyone wanting to create their own device account creation or validation scripts.

What do you need in order to run the scripts?

- Remote PowerShell access to your organization's domain or tenant, Exchange servers, and Skype for Business servers.
- Admin credentials for your organization's domain or tenant, Exchange servers, and Skype for Business servers.

> **Note**
>
> Whether you're creating a new account or modifying an already-existing account, the validation script will verify that your device account is configured correctly. You should always run the validation script before adding a device account to Surface Hub.

Running the scripts

The account creation scripts will:

- Ask for administrator credentials.
- Create device accounts in your domain/tenant.
- Create or assign a Surface Hub-compatible ActiveSync policy to the device account(s).
- Set various attributes for the created account(s) in Exchange and Skype for Business.
- Assign licenses and permissions to the created account(s).

These are the attributes that are set by the scripts:

Cmdlet	Attribute	Value
Set-Mailbox	RoomMailboxPassword	User-provided

Cmdlet	Attribute	Value
	EnableRoomMailboxAccount	True
	Type	Room
Set-CalendarProcessing	AutomateProcessing	AutoAccept
	RemovePrivateProperty	False
	DeleteSubject	False
	DeleteComments	False
	AddOrganizerToSubject	False
	AddAdditionalResponse	True
	AdditionalResponse	"This is a Surface Hub room!"
New-MobileDeviceMailboxPolicy	PasswordEnabled	False
	AllowNonProvisionableDevices	True
Enable-CSMeetingRoom	RegistrarPool	User-provided
	SipAddress	Set to the User Principal Name (UPN) of the device account
Set-MsolUserLicense (O365 only)	AddLicenses	User-provided
Set-MsolUser (O365 only)	PasswordNeverExpires	True
Set-AdUser (On-prem only)	Enabled	True
Set-AdUser (On-prem only)	PasswordNeverExpires	True

Account creation scripts

These scripts will create a device account for you. You can use the Account verification script to make sure they ran correctly.

The account creation scripts cannot modify an already existing account, but can be used to help you understand which cmdlets need to be run to configure the existing account correctly.

Create an on-premises account

PowerShell

```powershell
# SHAccountCreateOnPrem.ps1

$Error.Clear()
$ErrorActionPreference = "Stop"
$status = @{}

# Cleans up set state such as remote powershell sessions
function Cleanup()
{
    if ($sessExchange)
    {
        Remove-PSSession $sessExchange
    }
    if ($sessCS)
    {
        Remove-PSSession $sessCS
    }
}

function PrintError($strMsg)
{
    Write-Host $strMsg -foregroundcolor Red
}

function PrintSuccess($strMsg)
{
    Write-Host $strMsg -foregroundcolor Green
}

function PrintAction($strMsg)
{
    Write-Host $strMsg -ForegroundColor Cyan
}


# Cleans up and prints an error message
function CleanupAndFail($strMsg)
{
    if ($strMsg)
    {
        PrintError($strMsg);
    }
    Cleanup
    exit 1
}

# Exits if there is an error set and prints the given message
function ExitIfError($strMsg)
{
    if ($Error)
    {
        CleanupAndFail($strMsg);
```

```
    }
}

## Collect account data ##
$credNewAccount = (Get-Credential -Message "Enter the desired UPN and
password for this new account")
$strUpn = $credNewAccount.UserName
$strDisplayName = Read-Host "Please enter the display name you would like to
use for $strUpn"
if (!$credNewAccount -Or [System.String]::IsNullOrEmpty($strDisplayName) -Or
[System.String]::IsNullOrEmpty($credNewAccount.UserName) -Or
$credNewAccount.Password.Length -le 0)
{
    CleanupAndFail "Please enter all of the requested data to continue."
    exit 1
}

## Sign in to remote powershell for exchange and lync online ##

$credExchange = $null
$credExchange=Get-Credential -Message "Enter credentials of an Exchange user
with mailbox creation rights"
if (!$credExchange)
{
    CleanupAndFail("Valid credentials are required to create and prepare the
account.");
}
$strExchangeServer = Read-Host "Please enter the FQDN of your exchange
server (e.g. exch.contoso.com)"

# Lync info
$credLync = Get-Credential -Message "Enter credentials of a Skype for
Business admin (or cancel if they are the same as Exchange)"
if (!$credLync)
{
    $credLync = $credExchange
}
$strLyncFQDN = Read-Host "Please enter the FQDN of your Lync server (e.g.
lync.contoso.com) or enter to use [$strExchangeServer]"
if ([System.String]::IsNullOrEmpty($strLyncFQDN))
{
    $strLyncFQDN = $strExchangeServer
}


PrintAction "Connecting to remote sessions. This can occasionally take a
while - please do not enter input..."
try
{
    $sessExchange = New-PSSession -ConfigurationName microsoft.exchange -
Credential $credExchange -AllowRedirection -Authentication Kerberos -
ConnectionUri "http://$strExchangeServer/powershell" -WarningAction
SilentlyContinue
}
catch
```

```
{
    CleanupAndFail("Failed to connect to exchange. Please check your
credentials and try again. If this continues to fail, you may not have
permission for remote powershell - if not, please perform the setup
manually. Error message: $_")
}
PrintSuccess "Connected to Remote Exchange Shell"

try
{
    $sessLync = New-PSSession -Credential $credLync -ConnectionURI
"https://$strLyncFQDN/OcsPowershell" -AllowRedirection -WarningAction
SilentlyContinue
}
catch
{
    CleanupAndFail("Failed to connect to Lync. Please check your credentials
and try again. Error message: $_")
}
PrintSuccess "Connected to Lync Server Remote PowerShell"


Import-PSSession $sessExchange -AllowClobber -WarningAction SilentlyContinue
Import-PSSession $sessLync -AllowClobber -WarningAction SilentlyContinue

## Create the Exchange mailbox ##
> [!Note]
> These exchange commandlets do not always throw their errors as exceptions

# Because Get-Mailbox will throw an error if the mailbox is not found
$Error.Clear()
PrintAction "Creating a new account..."
try
{
    $mailbox = $null
    $mailbox = (New-Mailbox -UserPrincipalName $credNewAccount.UserName -
Alias
$credNewAccount.UserName.substring(0,$credNewAccount.UserName.indexOf('@'))
-room -Name $strDisplayName -RoomMailboxPassword $credNewAccount.Password -
EnableRoomMailboxAccount $true)
} catch { }
ExitIfError "Failed to create a new mailbox on exchange.";
$status["Mailbox Setup"] = "Successfully created a mailbox for the new
account"


$strEmail = $mailbox.WindowsEmailAddress
PrintSuccess "The following mailbox has been created for this room:
$strEmail"

## Create or retrieve a policy that will be applied to surface hub devices
##
# The policy disables requiring a device password so that the SurfaceHub
does not need to be lockable to use Active Sync
$strPolicy = Read-Host 'Please enter the name for a new Surface Hub
```

```
ActiveSync policy that will be created and applied to this account.
We will configure that policy to be compatible with Surface Hub devices.
If this script has been used before, please enter the name of the existing
policy.'

$easpolicy = $null
try {
    $easpolicy = Get-MobileDeviceMailboxPolicy $strPolicy
}
catch {}

if ($easpolicy)
{
    if (!$easpolicy.PasswordEnabled -and
($easpolicy.AllowNonProvisionableDevices -eq $null -or
$easpolicy.AllowNonProvisionableDevices ))
    {
        PrintSuccess "An existing policy has been found and will be applied
to this account."
    }
    else
    {
        PrintError "The policy you provided is incompatible with the surface
hub."
        $easpolicy = $null
        $status["Device Password Policy"] = "Failed to apply the EAS policy
to the account because the policy was invalid."
    }
}
else
{
    $Error.Clear()
    PrintAction "Creating policy..."
    $easpolicy = New-MobileDeviceMailboxPolicy -Name $strPolicy -
PasswordEnabled $false -AllowNonProvisionableDevices $true
    if ($easpolicy)
    {
        PrintSuccess "A new device policy has been created; you can use this
same policy for all future Surface Hub device accounts."
    }
    else
    {
        PrintError "Could not create $strPolicy"
    }
}

if ($easpolicy)
{
    # Convert mailbox to user type so we can apply the policy (necessary)
    # Sometimes it takes a while for this change to take affect so we have
some nasty retry loops
    $Error.Clear();
    try
    {
        Set-Mailbox $credNewAccount.UserName -Type Regular
```

```
    } catch {}
    if ($Error)
    {
        $Error.Clear()
        $status["Device Password Policy"] = "Failed to apply the EAS policy
to the account."
    }
    else
    {
        # Loop until resource type goes away, up to 5 times
        for ($i = 0; $i -lt 5 -And (Get-Mailbox
$credNewAccount.UserName).ResourceType; $i++)
        {
            Start-Sleep -s 5
        }
        # If the mailbox is still a Room we cannot apply the policy
        if (!((Get-Mailbox $credNewAccount.UserName).ResourceType))
        {
            $Error.Clear()
            # Set policy for account
            Set-CASMailbox $credNewAccount.UserName -ActiveSyncMailboxPolicy
$strPolicy
            if (!$Error)
            {
                $status["ActiveSync Policy"] = "Successfully applied
$strPolicy to the account"
            }
            else
            {
                $status["ActiveSync Policy"] = "Failed to apply the EAS
policy to the account."
            }
            $Error.Clear()

            # Convert back to room mailbox
            Set-Mailbox $credNewAccount.UserName -Type Room
            # Loop until resource type goes back to room
            for ($i = 0; ($i -lt 5) -And ((Get-Mailbox
$credNewAccount.UserName).ResourceType -ne "Room"); $i++)
            {
                Start-Sleep -s 5
            }
            if ((Get-Mailbox $credNewAccount.UserName).ResourceType -ne
"Room")
            {
                # A failure to convert the mailbox back to a room is
unfortunate but means the mailbox is unusable.
                $status["Mailbox Setup"] = "A mailbox was created but we
could not set it to a room resource type."
            }
            else
            {
                try
                {
                    Set-Mailbox $credNewAccount.UserName -
```

```
RoomMailboxPassword $credNewAccount.Password -EnableRoomMailboxAccount $true
                } catch { }
                if ($Error)
                {
                    $status["Mailbox Setup"] = "A room mailbox was created
but we could not set its password."
                }
                $Error.Clear()
            }

        }
    }
}
PrintSuccess "Account creation completed."

PrintAction "Setting calendar processing rules..."

$Error.Clear();
## Prepare the calendar for automatic meeting responses ##
try {
    Set-CalendarProcessing -Identity $credNewAccount.UserName -
AutomateProcessing AutoAccept
} catch { }
if ($Error)
{
    $status["Calendar Acceptance"] = "Failed to configure the account to
automatically accept/decline meeting requests"
}
else
{
    $status["Calendar Acceptance"] = "Successfully configured the account to
automatically accept/decline meeting requests"
}


$Error.Clear()
try {
    Set-CalendarProcessing -Identity $credNewAccount.UserName -
RemovePrivateProperty $false -AddOrganizerToSubject $false -
AddAdditionalResponse $true -DeleteSubject $false -DeleteComments $false -
AdditionalResponse "This is a Surface Hub room!"
} catch { }
if ($Error)
{
    $status["Calendar Response Configuration"] = "Failed to configure the
account's response properties"
}
else
{
    $status["Calendar Response Configuration"] = "Successfully configured
the account's response properties"
}

$Error.Clear()
## Configure the Account to not expire ##
```

```
PrintAction "Configuring password not to expire..."
Start-Sleep -s 20
try
{
    Set-AdUser $mailbox.UserPrincipalName -PasswordNeverExpires $true -
Enabled $true
}
catch
{

}

if ($Error)
{
    $status["Password Expiration Policy"] = "Failed to set the password to
never expire"
}
else
{
    $status["Password Expiration Policy"] = "Successfully set the password
to never expire"
}

PrintSuccess "Completed Exchange configuration"

## Setup Skype for Business. This is somewhat optional and if it fails we
SfbEnable can be used later ##
PrintAction "Configuring account for Skype for Business."

# Getting registrar pool
$strRegPool = $strLyncFQDN
$Error.Clear()
$strRegPoolEntry = Read-Host "Enter a Skype for Business Registrar Pool, or
leave blank to use [$strRegPool]"
if (![System.String]::IsNullOrEmpty($strRegPoolEntry))
{
    $strRegPool = $strRegPoolEntry
}

# Try to SfB-enable the account. Note that it may not work right away as the
account needs to propagate to active directory
PrintAction "Enabling Skype for Business..."
Start-Sleep -s 10
$Error.Clear()
try {
    Enable-CsMeetingRoom -Identity $credNewAccount.UserName -RegistrarPool
$strRegPool -SipAddressType EmailAddress
}
catch { }

if ($Error)
{
    $status["Skype for Business Account Setup"] = "Failed to setup the Skype
for Business meeting room - you can run EnableSfb.ps1 to try again."
    $Error.Clear();
```

```
}
else
{
    $status["Skype for Business Account Setup"] = "Successfully enabled
account as a Skype for Business meeting room"
}

Write-Host

## Cleanup and print results ##
Cleanup
$strDisplay = $mailbox.DisplayName
$strUsr = $credNewAccount.UserName
PrintAction "Summary for creation of $strUsr ($strDisplay)"
if ($status.Count -gt 0)
{
    ForEach($k in $status.Keys)
    {
        $v = $status[$k]
        $color = "yellow"
        if ($v[0] -eq "S") { $color = "green" }
        elseif ($v[0] -eq "F")
        {
            $color = "red"
            $v += " Go to https://aka.ms/shubtshoot"
        }

        Write-Host -NoNewline $k -ForegroundColor $color
        Write-Host -NoNewline ": "
        Write-Host $v
    }
}
else
{
    PrintError "The account could not be created"
}
```

Create a device account using Office 365

Creates an account as described in Create a device account using Office 365.

PowerShell

```
# SHAccountCreateO365.ps1

$Error.Clear()
$ErrorActionPreference = "Stop"
$status = @{}

# Cleans up set state such as remote powershell sessions
function Cleanup()
{
```

```
    if ($sessExchange)
    {
        Remove-PSSession $sessExchange
    }
    if ($sessCS)
    {
        Remove-PSSession $sessCS
    }
}

function PrintError($strMsg)
{
    Write-Host $strMsg -foregroundcolor Red
}

function PrintSuccess($strMsg)
{
    Write-Host $strMsg -foregroundcolor Green
}

function PrintAction($strMsg)
{
    Write-Host $strMsg -ForegroundColor Cyan
}


# Cleans up and prints an error message
function CleanupAndFail($strMsg)
{
    if ($strMsg)
    {
        PrintError($strMsg);
    }
    Cleanup
    exit 1
}

# Exits if there is an error set and prints the given message
function ExitIfError($strMsg)
{
    if ($Error)
    {
        CleanupAndFail($strMsg);
    }
}


## Check dependencies ##
try {
    Import-Module SkypeOnlineConnector
    Import-Module MSOnline
}
catch
{
    PrintError "Some dependencies are missing"
```

```
    PrintError "Please install the Windows PowerShell Module for Lync
Online. For more information go to
https://www.microsoft.com/download/details.aspx?id=39366"
    PrintError "Please install the Azure Active Directory module for
PowerShell from https://go.microsoft.com/fwlink/p/?linkid=236297"
    CleanupAndFail
}



## Collect account data ##
$credNewAccount = (Get-Credential -Message "Enter the desired UPN and
password for this new account")
$strUpn = $credNewAccount.UserName
$strDisplayName = Read-Host "Please enter the display name you would like to
use for $strUpn"
if (!$credNewAccount -Or [System.String]::IsNullOrEmpty($strDisplayName) -Or
[System.String]::IsNullOrEmpty($credNewAccount.UserName) -Or
$credNewAccount.Password.Length -le 0)
{
    CleanupAndFail "Please enter all of the requested data to continue."
    exit 1
}


## Sign in to remote powershell for exchange and lync online ##
$credAdmin = $null
$credAdmin=Get-Credential -Message "Enter credentials of an Exchange and
Skype for Business admin"
if (!$credadmin)
{
    CleanupAndFail "Valid admin credentials are required to create and
prepare the account."
}
PrintAction "Connecting to remote sessions. This can occasionally take a
while - please do not enter input..."
try
{
    $sessExchange = New-PSSession -ConfigurationName microsoft.exchange -
Credential $credAdmin -AllowRedirection -Authentication basic -ConnectionUri
"https://outlook.office365.com/powershell-liveid/" -WarningAction
SilentlyContinue
}
catch
{
    CleanupAndFail "Failed to connect to exchange. Please check your
credentials and try again. Error message: $_"
}

try
{
    $sessCS = New-CsOnlineSession -Credential $credAdmin
}
catch
{
```

```
    CleanupAndFail "Failed to connect to Skype for Business Online
Datacenter. Please check your credentials and try again. Error message: $_"
}

try
{
    Connect-MsolService -Credential $credAdmin
}
catch
{
    CleanupAndFail "Failed to connect to Azure Active Directory. Please
check your credentials and try again. Error message: $_"
}

Import-PSSession $sessExchange -AllowClobber -WarningAction SilentlyContinue
Import-PSSession $sessCS -AllowClobber -WarningAction SilentlyContinue

## Create the Exchange mailbox ##
> [!Note]
> These exchange commandlets do not always throw their errors as exceptions

# Because Get-Mailbox will throw an error if the mailbox is not found
$Error.Clear()
PrintAction "Creating a new account..."
try
{
    $mailbox = $null
    $mailbox = (New-Mailbox -MicrosoftOnlineServicesID
$credNewAccount.UserName -room -Name $strDisplayName -RoomMailboxPassword
$credNewAccount.Password -EnableRoomMailboxAccount $true)
} catch { }
ExitIfError "Failed to create a new mailbox on exchange.";
$status["Mailbox Setup"] = "Successfully created a mailbox for the new
account"


$strEmail = $mailbox.WindowsEmailAddress
PrintSuccess "The following mailbox has been created for this room:
$strEmail"


## Create or retrieve a policy that will be applied to surface hub devices
##
# The policy disables requiring a device password so that the SurfaceHub
does not need to be lockable to use Active Sync
$strPolicy = Read-Host 'Please enter the name for a new Surface Hub
ActiveSync policy that will be created and applied to this account.
We will configure that policy to be compatible with Surface Hub devices.
If this script has been used before, please enter the name of the existing
policy.'

$easpolicy = $null
try {
    $easpolicy = Get-MobileDeviceMailboxPolicy $strPolicy
}
```

```
catch {}

if ($easpolicy)
{
    if (!$easpolicy.PasswordEnabled -and
($easpolicy.AllowNonProvisionableDevices -eq $null -or
$easpolicy.AllowNonProvisionableDevices ))
    {
        PrintSuccess "An existing policy has been found and will be applied
to this account."
    }
    else
    {
        PrintError "The policy you provided is incompatible with the surface
hub."
        $easpolicy = $null
        $status["ActiveSync Policy"] = "Failed to apply the EAS policy to
the account because the policy was invalid."
    }
}
else
{
    $Error.Clear()
    PrintAction "Creating policy..."
    $easpolicy = New-MobileDeviceMailboxPolicy -Name $strPolicy -
PasswordEnabled $false -AllowNonProvisionableDevices $true
    if ($easpolicy)
    {
        PrintSuccess "A new device policy has been created; you can use this
same policy for all future Surface Hub device accounts."
    }
    else
    {
        PrintError "Could not create $strPolicy"
    }
}

if ($easpolicy)
{
    # Convert mailbox to user type so we can apply the policy (necessary)
    # Sometimes it takes a while for this change to take affect so we have
some nasty retry loops
    $Error.Clear();
    try
    {
        Set-Mailbox $credNewAccount.UserName -Type Regular
    } catch {}
    if ($Error)
    {
        $Error.Clear()
        $status["Device Password Policy"] = "Failed to apply the EAS policy
to the account."
        PrintError "Failed to convert to regular account"
    }
    else
```

```
    {
        # Loop until resource type goes away, up to 5 times
        for ($i = 0; $i -lt 5 -And (Get-Mailbox
$credNewAccount.UserName).ResourceType; $i++)
        {
            Start-Sleep -s 5
        }
        # If the mailbox is still a Room we cannot apply the policy
        if (!((Get-Mailbox $credNewAccount.UserName).ResourceType))
        {
            $Error.Clear()
            # Set policy for account
            Set-CASMailbox $credNewAccount.UserName -ActiveSyncMailboxPolicy
$strPolicy
            if (!$Error)
            {
                $status["Device Password Policy"] = "Successfully applied
$strPolicy to the account"
            }
            else
            {
                $status["Device Password Policy"] = "Failed to apply the EAS
policy to the account."
                PrintError "Failed to apply policy"
            }
            $Error.Clear()

            # Convert back to room mailbox
            Set-Mailbox $credNewAccount.UserName -Type Room
            # Loop until resource type goes back to room
            for ($i = 0; ($i -lt 5) -And ((Get-Mailbox
$credNewAccount.UserName).ResourceType -ne "Room"); $i++)
            {
                Start-Sleep -s 5
            }
            if ((Get-Mailbox $credNewAccount.UserName).ResourceType -ne
"Room")
            {
                # A failure to convert the mailbox back to a room is
unfortunate but means the mailbox is unusable.
                $status["Mailbox Setup"] = "A mailbox was created but we
could not set it to a room resource type."
            }
            else
            {
                Set-Mailbox $credNewAccount.UserName -RoomMailboxPassword
$credNewAccount.Password -EnableRoomMailboxAccount $true
                if ($Error)
                {
                    $status["Mailbox Setup"] = "A room mailbox was created
but we could not set its password."
                }
                $Error.Clear()
            }
```

```
        }
    }
}
else
{
    $status["Device Password Policy"] = "Failed to apply the EAS policy to
the account."
    PrintError "Failed to obtain policy"
}
PrintSuccess "Account creation completed."

PrintAction "Setting calendar processing rules..."

$Error.Clear();
## Prepare the calendar for automatic meeting responses ##
try {
    Set-CalendarProcessing -Identity $credNewAccount.UserName -
AutomateProcessing AutoAccept
} catch { }
if ($Error)
{
    $status["Calendar Acceptance"] = "Failed to configure the account to
automatically accept/decline meeting requests"
}
else
{
    $status["Calendar Acceptance"] = "Successfully configured the account to
automatically accept/decline meeting requests"
}


$Error.Clear()
try {
    Set-CalendarProcessing -Identity $credNewAccount.UserName -
RemovePrivateProperty $false -AddOrganizerToSubject $false -
AddAdditionalResponse $true -DeleteSubject $false -DeleteComments $false -
AdditionalResponse "This is a Surface Hub room!"
} catch { }
if ($Error)
{
    $status["Calendar Response Configuration"] = "Failed to configure the
account's response properties"
}
else
{
    $status["Calendar Response Configuration"] = "Successfully configured
the account's response properties"
}

$Error.Clear()
## Configure the Account to not expire ##
PrintAction "Configuring password not to expire..."
try
{
    Set-MsolUser -UserPrincipalName $credNewAccount.UserName -
```

```
PasswordNeverExpires $true
}
catch
{

}

if ($Error)
{
    $status["Password Expiration Policy"] = "Failed to set the password to
never expire"
}
else
{
    $status["Password Expiration Policy"] = "Successfully set the password
to never expire"
}

PrintSuccess "Completed Exchange configuration"

## Setup Skype for Business. This is somewhat optional and if it fails we
SfbEnable can be used later ##
PrintAction "Configuring account for Skype for Business."

# Getting registrar pool
$strRegPool = $null
try {
    $strRegPool = (Get-CsTenant).TenantPoolExtension
}
catch {}
$Error.Clear()
if (![System.String]::IsNullOrEmpty($strRegPool))
{
    $strRegPool = $strRegPool.Substring($strRegPool[0].IndexOf(':') + 1)
}
<#
$strRegPoolEntry = Read-Host "Enter a Skype for Business Registrar Pool, or
leave blank to use [$strRegPool]"
if (![System.String]::IsNullOrEmpty($strRegPoolEntry))
{
    $strRegPool = $strRegPoolEntry
}
#>

# Try to SfB-enable the account. Note that it may not work right away as the
account needs to propagate to active directory
PrintAction "Enabling Skype for Business on $strRegPool"
Start-Sleep -s 10
$Error.Clear()
try {
    Enable-CsMeetingRoom -Identity $credNewAccount.UserName -RegistrarPool
$strRegPool -SipAddressType EmailAddress
}
catch { }
```

```
if ($Error)
{
    $status["Skype for Business Account Setup"] = "Failed to setup the Skype
for Business meeting room - you can run EnableSfb.ps1 to try again."
    $Error.Clear();
}
else
{
    $status["Skype for Business Account Setup"] = "Successfully enabled
account as a Skype for Business meeting room"
}

## Now we need to assign a Skype for Business license to the account ##
# Assign a license to thes
$countryCode = (Get-CsTenant).CountryAbbreviation
$loc = Read-Host "Please enter the usage location for this device account
(where the account is being used). This is a 2-character code that is used
to assign licenses (e.g. $countryCode)"
try {
    $Error.Clear()
    Set-MsolUser -UserPrincipalName $credNewAccount.UserName -UsageLocation
$loc
}
catch{}
if ($Error)
{
    $status["Office 365 License"] = "Failed to assign an Office 365 license
to the account"
    $Error.Clear()
}
else
{
    PrintAction "We found the following licenses available for your tenant:"
    $skus = (Get-MsolAccountSku | Where-Object {
!$_.AccountSkuID.Contains("INTUNE"); })
    $i = 1
    $skus | % {
     Write-Host -NoNewline $i
     Write-Host -NoNewLine ": AccountSKUID: "
     Write-Host -NoNewLine $_.AccountSkuid
     Write-Host -NoNewLine " Active Units: "
     Write-Host -NoNewLine $_.ActiveUnits
     Write-Host -NoNewLine " Consumed Units: "
     Write-Host $_.ConsumedUnits
     $i++
    }
    $iLicenseIndex = 0;
    do
    {
        $iLicenseIndex = Read-Host 'Choose the number for the SKU you want
to pick'
    } while ($iLicenseIndex -lt 1 -or $iLicenseIndex -gt $skus.Length)
    $strLicenses = $skus[$iLicenseIndex - 1].AccountSkuId

    if (![System.String]::IsNullOrEmpty($strLicenses))
```

```
    {
        try
        {
            $Error.Clear()
            Set-MsolUserLicense -UserPrincipalName $credNewAccount.UserName
-AddLicenses $strLicenses
        }
        catch
        {

        }
        if ($Error)
        {
            $Error.Clear()
            $status["Office 365 License"] = "Failed to add a license to the
account. Make sure you have remaining licenses."
        }
        else
        {
            $status["Office 365 License"] = "Successfully added license to
the account"
        }
    }
    else
    {
        $status["Office 365 License"] = "You opted not to install a license
on this account"
    }
}


Write-Host

## Cleanup and print results ##
Cleanup
$strDisplay = $mailbox.DisplayName
$strUsr = $credNewAccount.UserName
PrintAction "Summary for creation of $strUsr ($strDisplay)"
if ($status.Count -gt 0)
{
    ForEach($k in $status.Keys)
    {
        $v = $status[$k]
        $color = "yellow"
        if ($v[0] -eq "S") { $color = "green" }
        elseif ($v[0] -eq "F")
        {
            $color = "red"
            $v += " Go to https://aka.ms/shubtshoot for help"
        }

        Write-Host -NoNewline $k -ForegroundColor $color
        Write-Host -NoNewline ": "
        Write-Host $v
    }
```

```
}
else
{
    PrintError "The account could not be created"
}
```

Account verification script

This script validates the previously created device account on Surface Hub and Surface Hub 2S, no matter which method was used to create it. This script is basically pass/fail. If one of the test errors out, it will show a detailed error message, but if all tests pass, the end result will be a summary report. For example, you might see:

Console

```
15 tests executed
0 failures
2 warnings
15 passed
```

Details of specific settings will not be shown.

PowerShell

```
# SHAccountValidate.ps1

$Error.Clear()
$ErrorActionPreference = "Stop"


# Cleans up set state such as remote powershell sessions
function Cleanup()
{
    if ($sessEx)
    {
        Remove-PSSession $sessEx
    }
    if ($sessSfb)
    {
        Remove-PSSession $sessSfb
    }
}

function PrintError($strMsg)
{
    Write-Host $strMsg -foregroundcolor "red"
}

function PrintSuccess($strMsg)
```

```
{
    Write-Host $strMsg -foregroundcolor "green"
}

function PrintAction($strMsg)
{
    Write-Host $strMsg -ForegroundColor Cyan
}


# Cleans up and prints an error message
function CleanupAndFail($strMsg)
{
    if ($strMsg)
    {
        PrintError($strMsg);
    }
    Cleanup
    exit 1
}

# Exits if there is an error set and prints the given message
function ExitIfError($strMsg)
{
    if ($Error)
    {
        CleanupAndFail($strMsg);
    }
}

$strUpn = Read-Host "What is the email address of the account you wish to
validate?"
if (!$strUpn.Contains('@'))
{
    CleanupAndFail "$strUpn is not a valid email address"
}
$strExServer = Read-Host "What is your exchange server? (leave blank for
online tenants)"
if ($strExServer.Equals(""))
{
    $fExIsOnline = $true
}
else
{
    $fExIsOnline = $false
}
$credEx = Get-Credential -Message "Please provide exchange user credentials"

$strRegistrarPool = Read-Host ("What is the Skype for Business registrar
pool for $strUpn" + "? (leave blank for online tenants)")
$fSfbIsOnline = $strRegistrarPool.Equals("")

$fHasOnPrem = $true
if ($fSfbIsOnline -and $fExIsOnline)
{
```

```
    do
    {
        $strHasOnPrem = (Read-Host "Do you have an on-premises Active
Directory (Y/N) (No if your domain services are hosted entirely
online)").ToUpper()
    } while ($strHasOnPrem -ne "Y" -and $strHasOnPrem -ne "N")
    $fHasOnPrem = $strHasOnPrem.Equals("Y")
}

$fHasOnline = $false
if ($fSfbIsOnline -or $fExIsOnline)
{
    $fHasOnline = $true
}

if ($fSfbIsOnline)
{
    try {
        Import-Module SkypeOnlineConnector
    }
    catch
    {
        CleanupAndFail "To verify Skype for Business in online tenants you
need the Lync Online Connector module from
https://www.microsoft.com/download/details.aspx?id=39366"
    }
}
else
{
    $credSfb = (Get-Credential -Message "Please enter Skype for Business
admin credentials")
}

if ($fHasOnline)
{
    $credSfb = $credEx
    try {
        Import-Module MSOnline
    }
    catch
    {
        CleanupAndFail "To verify accounts in online tenants you need the
Azure Active Directory module for PowerShell from
https://go.microsoft.com/fwlink/p/?linkid=236297"
    }
}

PrintAction "Connecting to Exchange Powershell Session..."
[System.Management.Automation.Runspaces.AuthenticationMechanism] $authType =
[System.Management.Automation.Runspaces.AuthenticationMechanism]::Kerberos
if ($fExIsOnline)
{
    $authType =
[System.Management.Automation.Runspaces.AuthenticationMechanism]::Basic
}
```

```
try
{
    $sessEx = $null
    if ($fExIsOnline)
    {
        $sessEx = New-PSSession -ConfigurationName microsoft.exchange -
Credential $credEx -AllowRedirection -Authentication $authType -
ConnectionUri "https://outlook.office365.com/powershell-liveid/" -
WarningAction SilentlyContinue
    }
    else
    {
        $sessEx = New-PSSession -ConfigurationName microsoft.exchange -
Credential $credEx -AllowRedirection -Authentication $authType -
ConnectionUri https://$strExServer/powershell -WarningAction
SilentlyContinue
    }
}
catch
{
}

if (!$sessEx)
{
    CleanupAndFail "Connecting to Exchange Powershell failed, please
validate your server is accessible and credentials are correct"
}

PrintSuccess "Connected to Exchange Powershell Session"

PrintAction "Connecting to Skype for Business Powershell Session..."

if ($fSfbIsOnline)
{
    $sessSfb = New-CsOnlineSession -Credential $credSfb
}
else
{
    $sessSfb = New-PSSession -Credential $credSfb -ConnectionURI
"https://$strRegistrarPool/OcsPowershell" -AllowRedirection -WarningAction
SilentlyContinue
}

if (!$sessSfb)
{
    CleanupAndFail "Connecting to Skype for Business Powershell failed,
please validate your server is accessible and credentials are correct"
}

PrintSuccess "Connected to Skype for Business Powershell"

if ($fHasOnline)
{
    $credMsol = $null
    if ($fExIsOnline)
```

```
    {
        $credMsol = $credEx
    }
    elseif ($fSfbIsOnline)
    {
        $credMsol = $credSfb
    }
    else
    {
        CleanupAndFail "Internal error - could not determine MS Online
credentials"
    }
    try
    {
        PrintAction "Connecting to Azure Active Directory Services..."
        Connect-MsolService -Credential $credMsol
        PrintSuccess "Connected to Azure Active Directory Services"
    }
    catch
    {
        # This really shouldn't happen unless there is a network error
        CleanupAndFail "Failed to connect to MSOnline"
    }
}


PrintAction "Importing remote sessions into the local session..."
try
{
    $importEx = Import-PSSession $sessEx -AllowClobber -WarningAction
SilentlyContinue -DisableNameChecking
    $importSfb = Import-PSSession $sessSfb -AllowClobber -WarningAction
SilentlyContinue -DisableNameChecking
}
catch
{
}
if (!$importEx -or !$importSfb)
{
    CleanupAndFail "Import failed"
}
PrintSuccess "Import successful"


$mailbox = $null
try
{
    $mailbox = Get-Mailbox -Identity $strUpn
}
catch
{
}

if (!$mailbox)
{
```

```
    CleanupAndFail "Account exists check failed. Unable to find the mailbox
for $strUpn - please make sure the Exchange account exists on $strExServer"
}

$exchange = $null
if (!$fExIsOnline)
{
    $exchange = Get-ExchangeServer
    if (!$exchange -or !$exchange.IsE14OrLater)
    {
        CleanupAndFail "A compatible exchange server version was not found.
Please use at least exchange 2010."
    }
}


$strAlias = $mailbox.UserPrincipalName
$strDisplayName = $mailbox.DisplayName

$strLinkedAccount = $strLinkedDomain = $strLinkedUser = $strLinkedServer =
$null
$credLinkedDomain = $Null
if (!$fExIsOnline -and !
[System.String]::IsNullOrEmpty($mailbox.LinkedMasterAccount) -and
!$mailbox.LinkedMasterAccount.EndsWith("\SELF"))
{
    $strLinkedAccount = $mailbox.LinkedMasterAccount
    $strLinkedDomain =
$strLinkedAccount.substring(0,$strLinkedAccount.IndexOf('\'))
    $strLinkedUser =
$strLinkedAccount.substring($strLinkedAccount.IndexOf('\') + 1)
    $strLinkedServer = Read-Host "What is the domain controller for the
$strLinkedDomain"
    $credLinkedDomain = (Get-Credential -Message "Please provide credentials
for $strLinkedDomain")
}









Write-Host
Write-Host
Write-Host
PrintAction "Performing verification checks on $strDisplayName..."
$Global:iTotalFailures = 0
$global:iTotalWarnings = 0
$Global:iTotalPasses = 0

function Validate()
{
    Param(
        [string]$Test,
```

```
        [bool]  $Condition,
        [string]$FailureMsg,
        [switch]$WarningOnly
    )

    Write-Host -NoNewline -ForegroundColor White $Test.PadRight(100,'.')
    if ($Condition)
    {
        Write-Host -ForegroundColor Green "Passed"
        $global:iTotalPasses++
    }
    else
    {
        if ($WarningOnly)
        {
            Write-Host -ForegroundColor Yellow ("Warning: "+$FailureMsg)
            $global:iTotalWarnings++
        }
        else
        {
            Write-Host -ForegroundColor Red ("Failed: "+$FailureMsg)
            $global:iTotalFailures++
        }
    }
}

## Exchange ##

Validate -WarningOnly -Test "The mailbox $strUpn is enabled as a room
account" -Condition ($mailbox.RoomMailboxAccountEnabled -eq $True) -
FailureMsg "RoomMailboxEnabled - without a device account, the Surface Hub
will not be able to use various key features."
$calendarProcessing = Get-CalendarProcessing -Identity $strUpn -
WarningAction SilentlyContinue -ErrorAction SilentlyContinue
Validate -Test "The mailbox $strUpn is configured to accept meeting
requests" -Condition ($calendarProcessing -ne $null -and
$calendarProcessing.AutomateProcessing -eq 'AutoAccept') -FailureMsg
"AutomateProcessing - the Surface Hub will not be able to send mail or sync
its calendar."
Validate -WarningOnly -Test "The mailbox $strUpn will not delete meeting
comments" -Condition ($calendarProcessing -ne $null -and
!$calendarProcessing.DeleteComments) -FailureMsg "DeleteComments - the
Surface Hub may be missing some meeting information on the welcome screen
and Skype."
Validate -WarningOnly -Test "The mailbox $strUpn keeps private meetings
private" -Condition ($calendarProcessing -ne $null -and
!$calendarProcessing.RemovePrivateProperty) -FailureMsg
"RemovePrivateProperty - the Surface Hub will make show private meetings."
Validate -Test "The mailbox $strUpn keeps meeting subjects" -Condition
($calendarProcessing -ne $null -and !$calendarProcessing.DeleteSubject) -
FailureMsg "DeleteSubject - the Surface Hub will not keep meeting subject
information."
Validate -WarningOnly -Test "The mailbox $strUpn does not prepend meeting
organizers to subjects" -Condition ($calendarProcessing -ne $null -and
!$calendarProcessing.AddOrganizerToSubject) -FailureMsg
```

```
"AddOrganizerToSubject - the Surface Hub will not display meeting subjects
as intended."

if ($fExIsOnline)
{
    #No online specifics
}
else
{
    #No onprem specifics
}

#ActiveSync
$casMailbox = Get-Casmailbox $strUpn -WarningAction SilentlyContinue -
ErrorAction SilentlyContinue
Validate -Test "The mailbox $strUpn has a mailbox policy" -Condition
($casMailbox -ne $null) -FailureMsg "PasswordEnabled - unable to find policy
- the Surface Hub will not be able to send mail or sync its calendar."
if ($casMailbox)
{
    $policy = $null
    if ($fExIsOnline -or $exchange.IsE15OrLater)
    {
        $strPolicy = $casMailbox.ActiveSyncMailboxPolicy
        $policy = Get-MobileDeviceMailboxPolicy -Identity $strPolicy -
WarningAction SilentlyContinue -ErrorAction SilentlyContinue
        Validate -Test "The policy $strPolicy does not require a device
password" -Condition ($policy.PasswordEnabled -ne $True) -FailureMsg
"PasswordEnabled - policy requires a device password - the Surface Hub will
not be able to send mail or sync its calendar."
    }
    else
    {
        $strPolicy = $casMailbox.ActiveSyncMailboxPolicy
        $policy = Get-ActiveSyncMailboxPolicy -Identity $strPolicy -
WarningAction SilentlyContinue -ErrorAction SilentlyContinue
        Validate -Test "The policy $strPolicy does not require a device
password" -Condition ($policy.PasswordEnabled -ne $True) -FailureMsg
"PasswordEnabled - policy requires a device password - the Surface Hub will
not be able to send mail or sync its calendar."
    }

    if ($policy -ne $null)
    {
        Validate -Test "The policy $strPolicy allows non-provisionable
devices" -Condition ($policy.AllowNonProvisionableDevices -eq $null -or
$policy.AllowNonProvisionableDevices -eq $true) -FailureMsg
"AllowNonProvisionableDevices - policy will not allow the SurfaceHub to
sync"
    }

}


# Check the default access level
```

```
$orgSettings = Get-ActiveSyncOrganizationSettings
$strDefaultAccessLevel = $orgSettings.DefaultAccessLevel
Validate -Test "ActiveSync devices are allowed" -Condition
($strDefaultAccessLevel -eq 'Allow') -FailureMsg "DeviceType Windows Mail is
accessible - devices are not allowed by default - the surface hub will not
be able to send mail or sync its calendar."

# Check if there exists a device access rule that bans the device type
Windows Mail
$blockingRules = Get-ActiveSyncDeviceAccessRule | where {($_.AccessLevel -eq
'Block' -or $_.AccessLevel -eq 'Quarantine') -and $_.Characteristic -eq
'DeviceType'-and $_.QueryString -eq 'WindowsMail'}
Validate -Test "Windows mail devices are not blocked or quarantined" -
Condition ($blockingRules -eq $null -or $blockingRules.Length -eq 0) -
FailureMsg "DeviceType Windows Mail is accessible - devices are blocked or
quarantined - the surface hub will not be able to send mail or sync its
calendar."

## End Exchange ##



## SfB ##
$strLyncIdentity = $null
if ($fSfbIsOnline)
{
    $strLyncIdentity = $strUpn
}
else
{
    $strLyncIdentity = $strAlias
}

$lyncAccount = $null
try {
    $lyncAccount = Get-CsMeetingRoom -Identity $strLyncIdentity -
WarningAction SilentlyContinue -ErrorAction SilentlyContinue
} catch {
    try {
        $lyncAccount = Get-CsUser -Identity $strLyncIdentity -WarningAction
SilentlyContinue -ErrorAction SilentlyContinue
    } catch { }
}
Validate -Test "There is a Lync or Skype for Business account for
$strLyncIdentity" -Condition ($lyncAccount -ne $null -and
$lyncAccount.Enabled) -FailureMsg "SfB Enabled - there is no Skype for
Business account - meetings will not support Skype for Business"
if ($lyncAccount)
{
    Validate -Test "The meeting room has a SIP address" -Condition (!
[System.String]::IsNullOrEmpty($lyncAccount.SipAddress)) -FailureMsg "SfB
Enabled - there is no SIP Address - the device account cannot be used to
sign into Skype for Business."
}
## End SFB ##
```

```
if ($fHasOnline)
{
    #License validation and password expiry
    $accountOnline = Get-MsolUser -UserPrincipalName $strUpn -WarningAction
SilentlyContinue -ErrorAction SilentlyContinue
    Validate -Test "There is an online user account for $strUpn" -Condition
($accountOnline -ne $null) -FailureMsg "Could not find a Microsoft Online
account for this user even though some services are online"
    if ($accountOnline)
    {
        Validate -Test "The password for $strUpn will not expire" -Condition
($accountOnline.PasswordNeverExpires -eq $True) -FailureMsg
"PasswordNeverExpires - the admin will need to update the device account's
password on the Surface Hub when it expires."
        if ($fIsSfbOnline -and !$fIsExOnline)
        {
            $strLicenseFailureMsg = "Has O365 license - The devices will not
be able to use Skype for Business services."
        }
        elseif ($fIsExOnline -and !$fIsSfbOnline)
        {
            $strLicenseFailureMsg = "Has O365 license - The devices will not
be able to use Exchange Online services."
        }
        else
        {
            $strLicenseFailureMsg = "Has O365 license - The devices will not
be able to use Skype for Business or Exchange Online services."
        }
        Validate -Test "$strUpn is licensed" -Condition
($accountOnline.IsLicensed -eq $True) -FailureMsg $strLicenseFailureMsg

        Validate -Test "$strUpn is allowed to sign in" -Condition
($accountOnline.BlockCredential -ne $True) -FailureMsg "BlockCredential -
This user is not allowed to sign in."
    }
}

#If there is an on-prem component, we can get the authoritative AD user from
mailbox
if ($fHasOnPrem)
{
    $accountOnPrem = $null
    if ($strLinkedAccount)
    {
        $accountOnPrem = Get-AdUser $strLinkedUser -server $strLinkedServer
-credential $credLinkedDomain -properties PasswordNeverExpires -
WarningAction SilentlyContinue -ErrorAction SilentlyContinue
    }
    else
    {
        #AD User enabled validation
        $accountOnPrem = Get-AdUser $mailbox.UserPrincipalName -properties
```

```
PasswordNeverExpires -WarningAction SilentlyContinue -ErrorAction
SilentlyContinue
    }
    $strOnPremUpn = $accountOnPrem.UserPrincipalName
    Validate -Test "There is a user account for $strOnPremUpn" -Condition
($accountOnprem -ne $null) -FailureMsg "Could not find an Active Directory
account for this user"
    if ($accountOnPrem)
    {
        Validate -WarningOnly -Test "The password for $strOnPremUpn will not
expire" -Condition ($accountOnprem.PasswordNeverExpires -eq $True) -
FailureMsg "PasswordNeverExpires - the admin will need to update the device
account's password on the Surface Hub when it expires."
        Validate -Test "$strOnPremUpn is enabled" -Condition
$accountOnPrem.Enabled -FailureMsg "AccountEnabled - this device account
will not sign in"
    }
}


$global:iTotalTests = ($global:iTotalFailures + $global:iTotalPasses +
$global:iTotalWarnings)

Write-Host -NoNewline $global:iTotalTests "tests executed: "
Write-Host -NoNewline -ForegroundColor Red $Global:iTotalFailures "failures
"
Write-Host -NoNewline -ForegroundColor Yellow $Global:iTotalWarnings
"warnings "
Write-Host -ForegroundColor Green $Global:iTotalPasses "passes "

Cleanup
```

Enable Skype for Business

This script will enable Skype for Business on a device account. Use it only if Skype for Business wasn't previously enabled during account creation.

PowerShell

```
## This script performs only the Enable for Skype for Business step on an
account. It should only be run if this step failed in SHAccountCreate and
the other steps have been completed ##
# EnableSfb.ps1

$Error.Clear()
$ErrorActionPreference = "Stop"

# Cleans up set state such as remote powershell sessions
function Cleanup()
{
    if ($sessCS)
```

```
    {
        Remove-PSSession $sessCS
    }
}

function PrintError($strMsg)
{
    Write-Host $strMsg -foregroundcolor "red"
}

function PrintSuccess($strMsg)
{
    Write-Host $strMsg -foregroundcolor "green"
}

# Cleans up and prints an error message
function CleanupAndFail($strMsg)
{
    if ($strMsg)
    {
        PrintError($strMsg);
    }
    Cleanup
    exit 1
}

# Exits if there is an error set and prints the given message
function ExitIfError($strMsg)
{
    if ($Error)
    {
        CleanupAndFail($strMsg);
    }
}

## Check dependencies ##

$input = Read-Host "Is the account you wish to enable part of an online
environment (enter O) or on-premises environment (enter P)"
if ($input -eq "P")
{
    $online = $false
}
elseif ($input -eq "O")
{
    $online = $true
}
else
{
    CleanupAndFail "Invalid selection"
}
if ($online)
{
    try {
        Import-Module SkypeOnlineConnector
```

```
    }
    catch
    {
        PrintError "Some dependencies are missing"
        PrintError "Please install the Windows PowerShell Module for Lync
Online. For more information go to
https://www.microsoft.com/download/details.aspx?id=39366"
        PrintError "Please install the Azure Active Directory module for
PowerShell from https://go.microsoft.com/fwlink/p/?linkid=236297"
        CleanupAndFail
    }
}
else
{
    $strRegPool = Read-Host "Enter the FQDN of your Skype for Business
Registrar Pool"
}


## Collect account data ##
Write-Host "-----------  Enter info for the account to enable  -----------."
-foregroundcolor "magenta"
$strRoomUri=Read-Host 'Please enter the UPN of the account you are enabling
(e.g. confroom@surfacehub.microsoft.com)'

if ([System.String]::IsNullOrEmpty($strRoomUri))
{
    CleanupAndFail "Please enter all of the requested data to continue."
    exit 1
}
Write-Host "------------------------------------------------------------."
-foregroundcolor "magenta"



## Sign in to remote powershell for exchange and lync online ##
Write-Host "`n------------------  Establishing connection  ----------------
-." -foregroundcolor "magenta"
$credAdmin=Get-Credential -Message "Enter credentials of a Skype for
Business admin"
if (!$credadmin)
{
    CleanupAndFail("Valid admin credentials are required to create and
prepare the account.");
}
Write-Host "Connecting to remote sessions. This can occasionally take a
while - please do not enter input..."

try
{
    if ($online)
    {
        $sessCS = New-CsOnlineSession -Credential $credAdmin
    }
    else
```

```
    {
        $sessCS = New-PSSession -Credential $credAdmin -ConnectionURI
"https://$strRegPool/OcsPowershell" -AllowRedirection -WarningAction
SilentlyContinue
    }
}
catch
{
    CleanupAndFail("Failed to connect to Skype for Business server. Please
check your credentials and try again. Error message: $_")
}

Import-PSSession $sessCS -AllowClobber


Write-Host "------------------------------------------------------------."
-foregroundcolor "magenta"

# Getting registrar pool
if ($online)
{
    try {
        $strRegPool = $null;
        $strRegPool = (Get-CsTenant).RegistrarPool
    } catch {}
    if ($Error)
    {
        $Error.Clear();
        $strRegPool = "";
        Write-Host "We failed to lookup your Skype for Business Registrar
Pool, but you can still enter it manually"
    }
    else
    {
        $strRegPool = $strRegPool[0].Substring($strRegPool[0].IndexOf(':') +
1)
    }
}


$Error.Clear()
try {
    Enable-CsMeetingRoom -Identity $strRoomUri -RegistrarPool $strRegPool -
SipAddressType EmailAddress
}
catch {}

ExitIfError("Failed to setup Skype for Business meeting room")

PrintSuccess "Successfully enabled $strRoomUri as a Skype for Business
meeting room"

Cleanup
```

Useful cmdlets

Creating a Surface Hub-compatible ActiveSync policy

For Surface Hub to use Exchange services, a device account configured with a compatible ActiveSync policy must be provisioned on the device. This policy has the following requirements:

```
syntax

PasswordEnabled == 0
```

In the following cmdlets, `$strPolicy` is the name of the ActiveSync policy, and `$strRoomUpn` is the UPN of the device account you want to apply the policy to.

Note that in order to run the cmdlets, you need to set up a remote PowerShell session and:

- Your admin account must be remote-PowerShell-enabled. This allows the admin to use the PowerShell cmdlets that are needed by the script. (This permission can be set using `set-user $admin -RemotePowerShellEnabled $true`)
- Your admin account must have the "Reset Password" role if you plan to run the creation scripts. This allows the admin to change the password of the account, which is needed for the script. The Reset Password Role can be enabled using the Exchange Admin Center.

Create the policy.

```
PowerShell

# Create new policy with PasswordEnabled == false
New-MobileDeviceMailboxPolicy -Name $strPolicy -PasswordEnabled $false –
AllowNonProvisionableDevices $true
```

To apply the policy, the mailbox cannot be a room type, so it has to be converted into a user first.

```
PowerShell

# Convert user to regular type
Set-Mailbox $strRoomUpn -Type Regular
# Set policy for account
Set-CASMailbox $strRoomUpn -ActiveSyncMailboxPolicy $strPolicy
```

Now the device account just needs to be converted back into a room type.

```PowerShell
# Convert back to room mailbox
Set-Mailbox $strRoomUpn -Type Room
```

Allowing device IDs for ActiveSync

To allow an account `$strRoomUpn`, run the following command:

```PowerShell
Set-CASMailbox –Identity $strRoomUpn –ActiveSyncAllowedDeviceIDs “<ID>”
```

To find a device's ID, run:

```PowerShell
Get-ActiveSyncDevice -Mailbox $strRoomUpn
```

This retrieves device information for every device that the account has been provisioned on, Including the `DeviceId` property.

Auto-accepting and declining meeting requests

For a device account to automatically accept or decline meeting requests based on its availability, the **AutomateProcessing** attribute must be set to **AutoAccept**. This is recommended as to prevent overlapping meetings.

```PowerShell
Set-CalendarProcessing $strRoomUpn -AutomateProcessing AutoAccept
```

Accepting external meeting requests

For a device account to accept external meeting requests (a meeting request from an account not in the same tenant/domain), the device account must be set to allow processing of external meeting requests. Once set, the device account will automatically accept or decline meeting requests from external accounts as well as local accounts.

> **Note**
>
> If the **AutomateProcessing** attribute is not set to **AutoAccept**, then setting this will have no effect.

PowerShell

```
Set-CalendarProcessing $strRoomUpn -ProcessExternalMeetingMessages $true
```

Downloadable resources for Surface Hub readiness

Article • 04/19/2023

This topic provides links to useful Surface Hub documents, such as product datasheets and user's guide.

Link	Description
Surface Hub Setup Guide (English, French, Spanish) (PDF)	Get a quick overview of how to set up the environment for your new Surface Hub.
Surface Hub Quick Reference Guide (PDF)	Use this quick reference guide to get information about key features and functions of the Surface Hub.
Surface Hub User Guide (PDF)	Learn how to use Surface Hub in scheduled or ad-hoc meetings. Invite remote participants, use the built-in tools, save data from your meeting, and more.
Surface Hub Replacement PC Drivers	The Surface Hub Replacement PC driver set is available for those customers who have chosen to disable the Surface Hub's internal PC and use an external computer with their 84" or 55" Surface Hub. This download is meant to be used with the Surface Hub Admin Guide , which contains further details on configuring a Surface Hub Replacement PC.
Microsoft Surface Hub Rollout and Adoption Success Kit (ZIP)	Best practices for generating awareness and implementing change management to maximize adoption, usage, and benefits of Microsoft Surface Hub. The Rollout and Adoption Success Kit zip file includes the Rollout and Adoption Success Kit detailed document, Surface Hub presentation, demo guidance, awareness graphics, and more.
Unpacking Guide for 84-inch Surface Hub (PDF)	Learn how to unpack your 84-inch Surface Hub efficiently and safely. Watch the video (opens in a pop-up media player)

Link	Description
Unpacking Guide for 55-inch Surface Hub (PDF)	Learn how to unpack your 55-inch Surface Hub efficiently and safely. Watch the video (opens in a pop-up media player)
Wall Mounting and Assembly Guide (PDF)	Detailed instructions on how to safely and securely assemble the wall brackets, and how to mount your Surface Hub onto them. Watch the video (opens in a pop-up media player)
Floor-Supported Mounting and Assembly Guide (PDF)	Detailed instructions on how to safely and securely assemble the floor-supported brackets, and how to mount your Surface Hub onto them. Watch the video (opens in a pop-up media player)
Rolling Stand Mounting and Assembly Guide (PDF)	Detailed instructions on how to safely and securely assemble the rolling stand, and how to mount your Surface Hub onto it. Watch the video (opens in a pop-up media player)
Mounts and Stands Datasheet (PDF)	Specifications and prices for all Surface Hub add-on stands and mounts that turn your workspace into a Surface Hub workspace.
Surface Hub Stand and Wall Mount Specifications (PDF)	Illustrated specifications for the 55" and 84" Surface Hub rolling stands, wall mounts, and floor-supported wall mounts.

Reset and recovery for Surface Hub (v1)

Article • 01/23/2023 • Applies to: Surface Hub

You can reset Surface Hub to restore the operating system to the last cumulative Windows update. The following information is removed:

- All local user files and configuration data.
- The device account.
- Account data for local administrators.
- Domain-join or Azure AD-join data.
- Mobile Device Management (MDM) enrollment data.
- Configuration data that was set by using MDM or the Settings app.

> **Tip**
>
> If the reset option cannot be used, the **Surface Hub Recovery Tool** can reimage the Surface Hub SSD directly.

Reset a Surface Hub

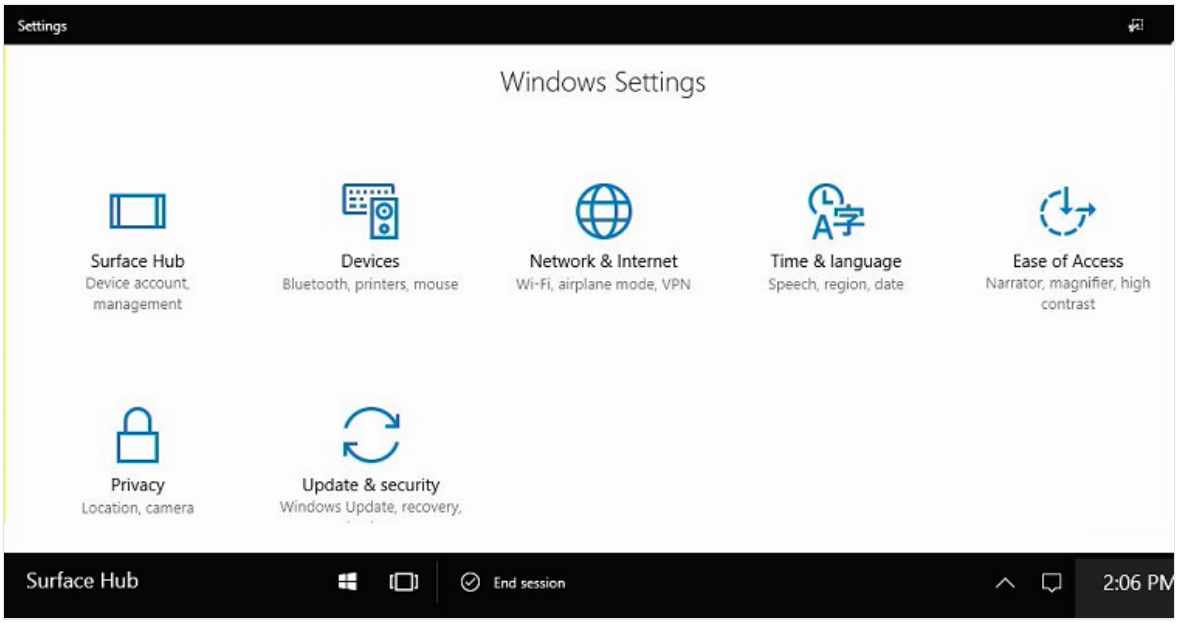
You may have to reset Surface Hub for the following scenarios:

- You're repurposing the device for a new meeting space and want to reconfigure it.
- You want to change how you locally manage the device.

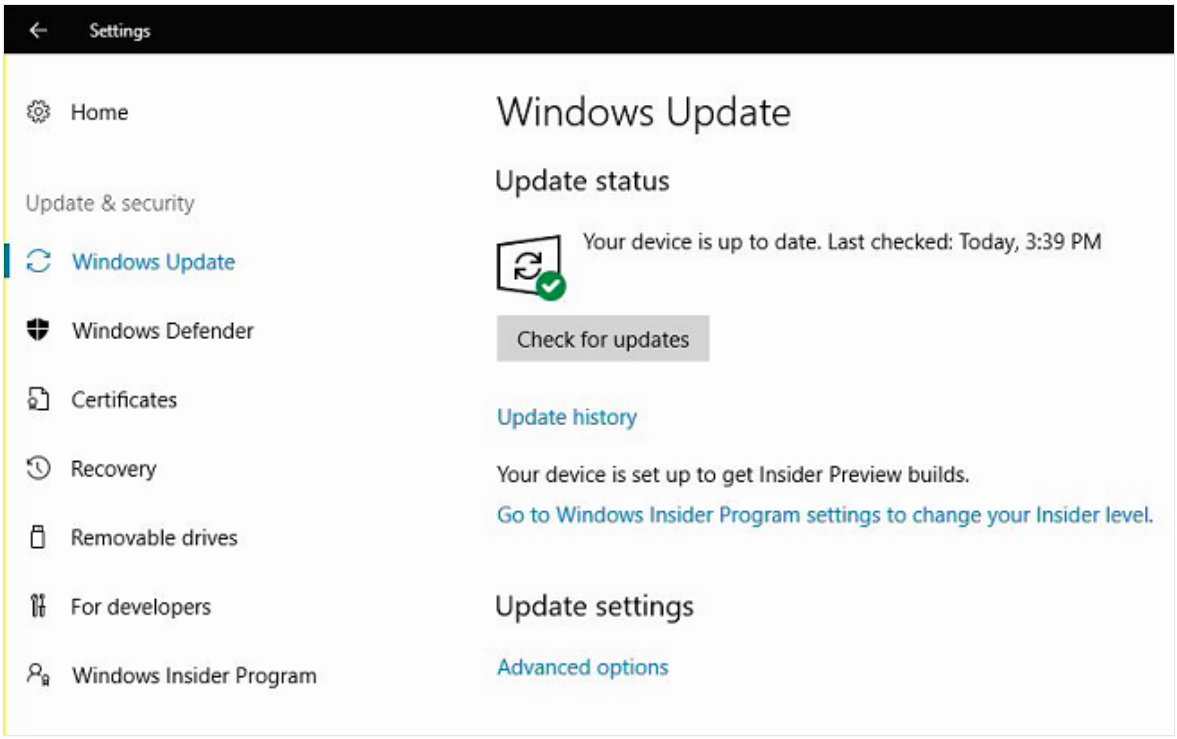
During the reset process, if you see a blank screen for long periods, wait and don't take any action.

> **⚠ Warning**
>
> The device reset process may take up to six hours. Do not turn off or unplug the Surface Hub until the process has finished. If you interrupt the process, the device becomes inoperable and requires warranty service to become functional again.

1. On your Surface Hub, open **Settings**.

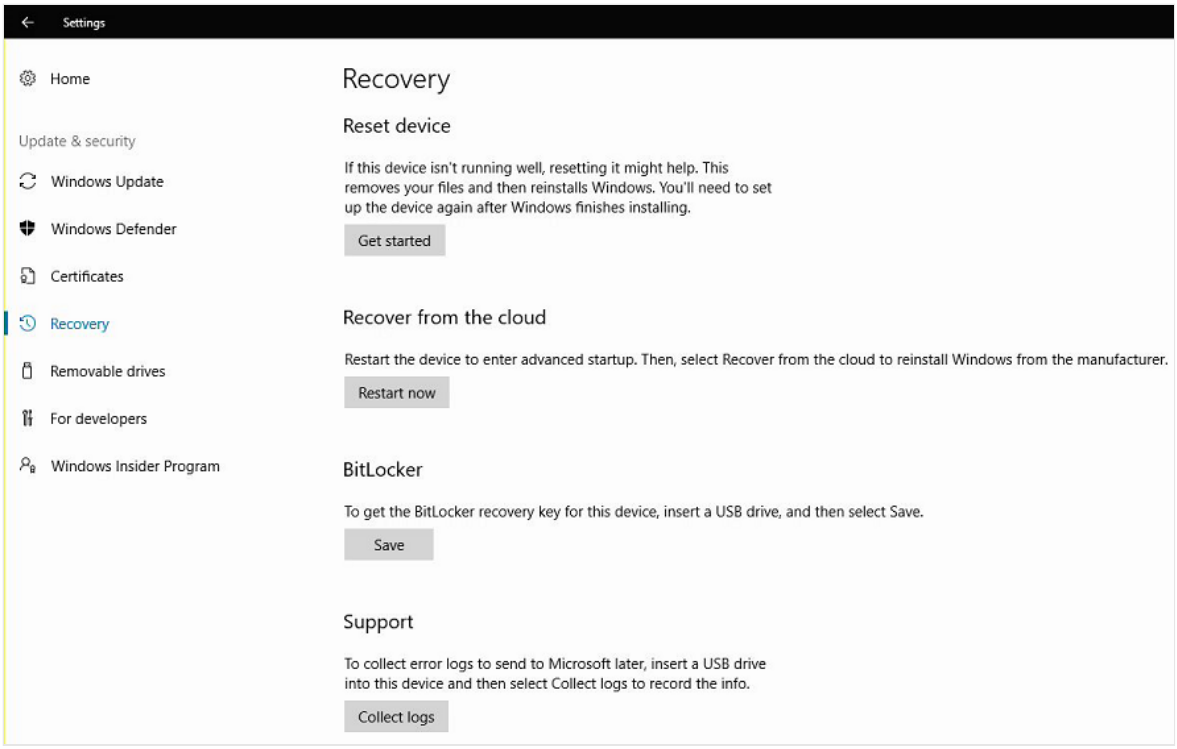


2. Select **Update & Security**.



3. Select **Recovery**, and then, under **Reset device**, select **Get started**.

> **ⓘ Important**
>
> Ensure that your BitLocker key is available as you will be prompted for it later. To learn more, see **Save your BitLocker key**. When the Hub reboots to the recovery partition, it will prompt you to enter the BitLocker key. Skipping that prompt will cause reset to fail.



After the reset process finishes, the Surface Hub starts the first run program again. If the reset process encounters a problem, it rolls the Surface Hub back to the previously existing operating system image and then displays the Welcome screen.

Recover a locked Surface Hub

If the Surface Hub becomes unusable and you can't reset it from the Settings app, you can still reset it if you have the BitLocker recovery key.

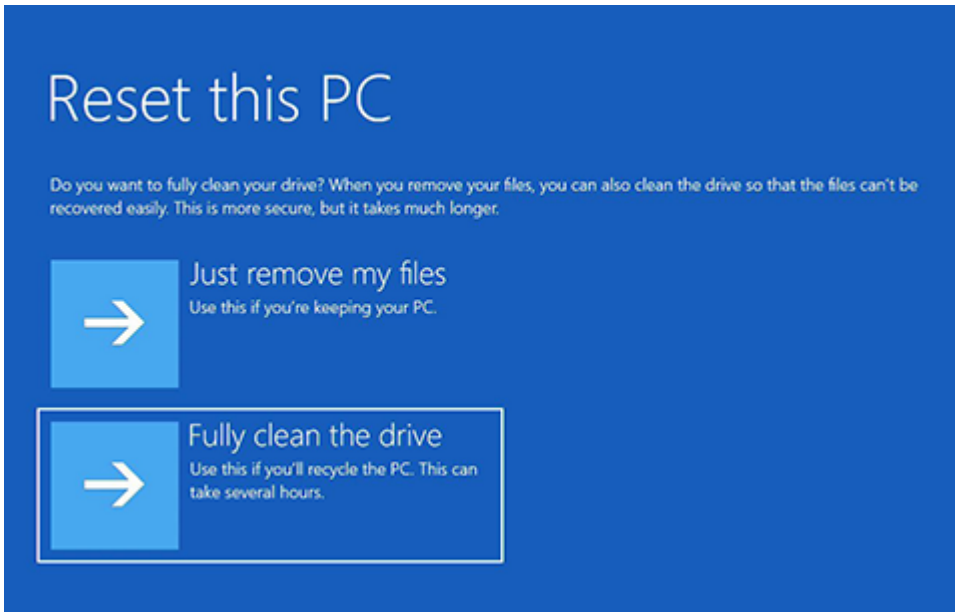
1. Locate the power switch on the bottom of Surface Hub. The power switch is next to the power cord connection. For more information about the power switch, see the Surface Hub Site Readiness Guide (PDF).

2. While the Surface Hub displays the Welcome screen, use the power switch to turn off the Surface Hub.

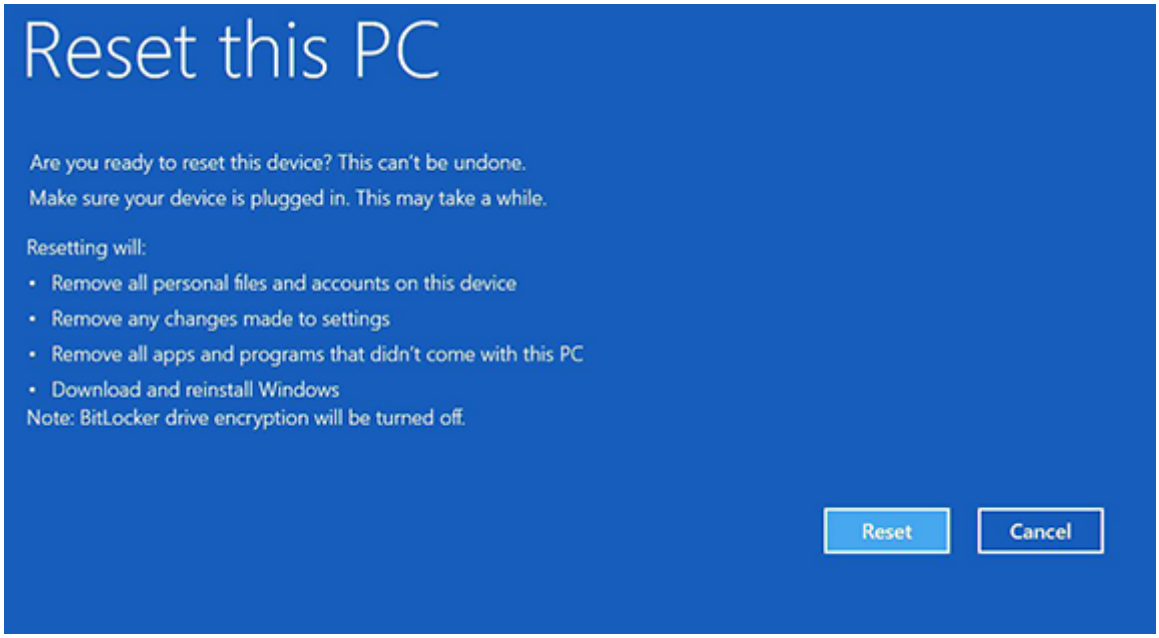
3. Use the power switch to turn the Surface Hub back on. The device starts and displays the Surface Hub Logo screen. When you see spinning dots under the Surface Hub Logo, use the power switch to turn the Surface Hub off again.

4. Repeat step 3 twice, or until Surface Hub displays the "Preparing Automatic Repair" message. After it displays this message, Surface Hub shows the Windows RE screen.

5. Select **Reset** > **Local reinstall** > **Fully clean the drive.**



6. You'll be asked **Are you ready to reset this device?**. Select **Reset**.



Contact Support

If you have questions or need help, you can create a support request.

Related articles

- Surface Hub Recovery Tool
- Manage Microsoft Surface Hub

Use the Surface Hub Recovery Tool

Article • 01/23/2023

The Microsoft Surface Hub Recovery Tool helps you reimage your Surface Hub Solid State Drive (SSD) from a separate PC without replacing the SSD or calling support. Use this tool for any of the following scenarios:

- You're unable to recover Surface Hub from the cloud.
- You need to reimage an SSD that that has an older version of the operating system.
- You no longer have access to the Administrator password.
- You're encountering boot errors that prevent restarting Surface Hub.

> **Note**
>
> The tool won't fix physically damaged SSDs.

To reimage the Surface Hub SSD using the Recovery Tool, you'll need to remove the SSD from the Surface Hub and connect the drive to the USB-to-SATA cable. Next, connect the cable to the desktop PC on which the Recovery Tool is installed. For more information on how to remove the existing drive from your Surface Hub, see Surface Hub SSD replacement.

> **Important**
>
> Do not let the device go to sleep or interrupt the download of the image file.

If the tool is unsuccessful in reimaging your drive, contact Surface Hub Support.

Prerequisites

Mandatory

- Host PC running 64-bit version of Windows 10, version 1607 or higher.
- Internet access
- Open USB 2.0 or greater port
- USB-to-SATA cable
- 10 GB of free disk space on the host computer

- SSDs shipped with Surface Hub or an SSD provided by Support as a replacement. SSDs not supplied by Microsoft aren't supported.

Recommended

- High-speed Internet connection
- Open USB 3.0 port
- USB 3.0 or higher USB-to-SATA cable
- The imaging tool was tested with the following make and model of cables:
  - Startech USB312SAT3CB
  - Rosewill RCUC16001
  - Ugreen 20231

Download Surface Hub Recovery Tool

Surface Hub Recovery Tool is available for download from Surface Hub Tools for IT under the file name **SurfaceHub_Recovery_v2.7.139.0.msi**.

To start the download, select **Download**, choose **SurfaceHub_Recovery_v2.7.139.0.msi** from the list, and select **Next**. From the pop-up, choose one of the following options:

- Select **Run** to start the installation immediately.
- Select **Save** to copy the download to your computer for later installation.

Install Surface Hub Recovery Tool on the host PC.

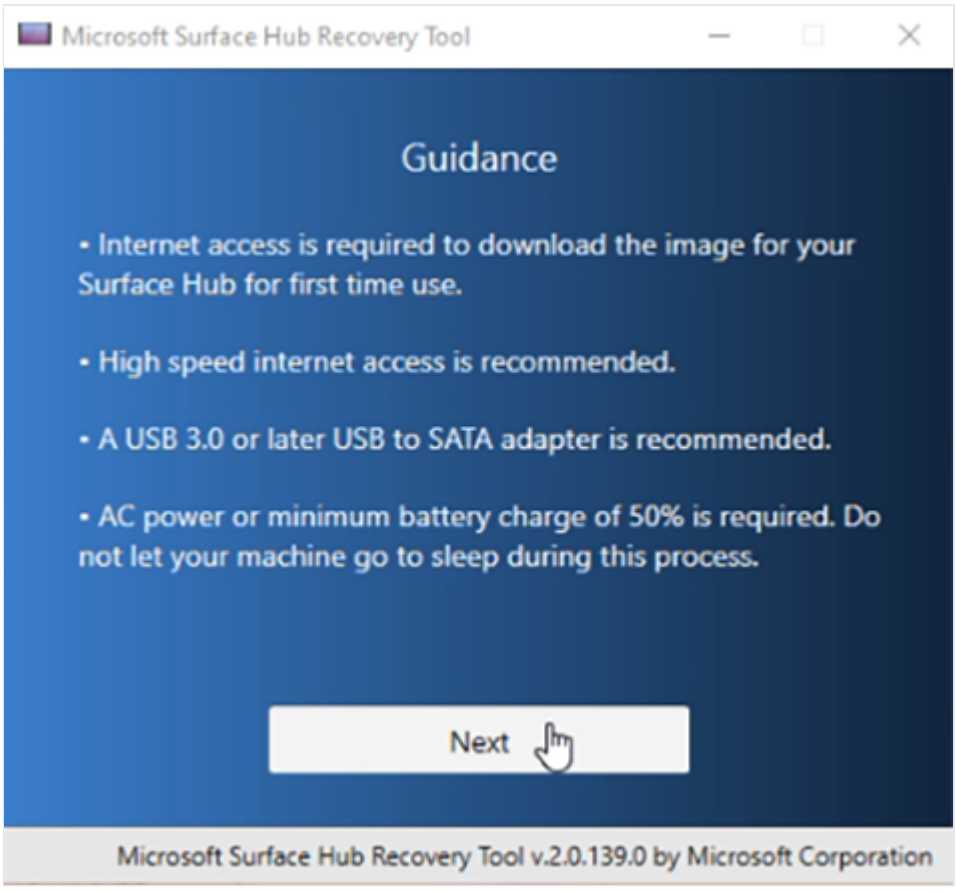
Run Surface Hub Recovery Tool

1. On the host PC, select the **Start** button, scroll through the alphabetical list on the left, and select the recovery tool shortcut.

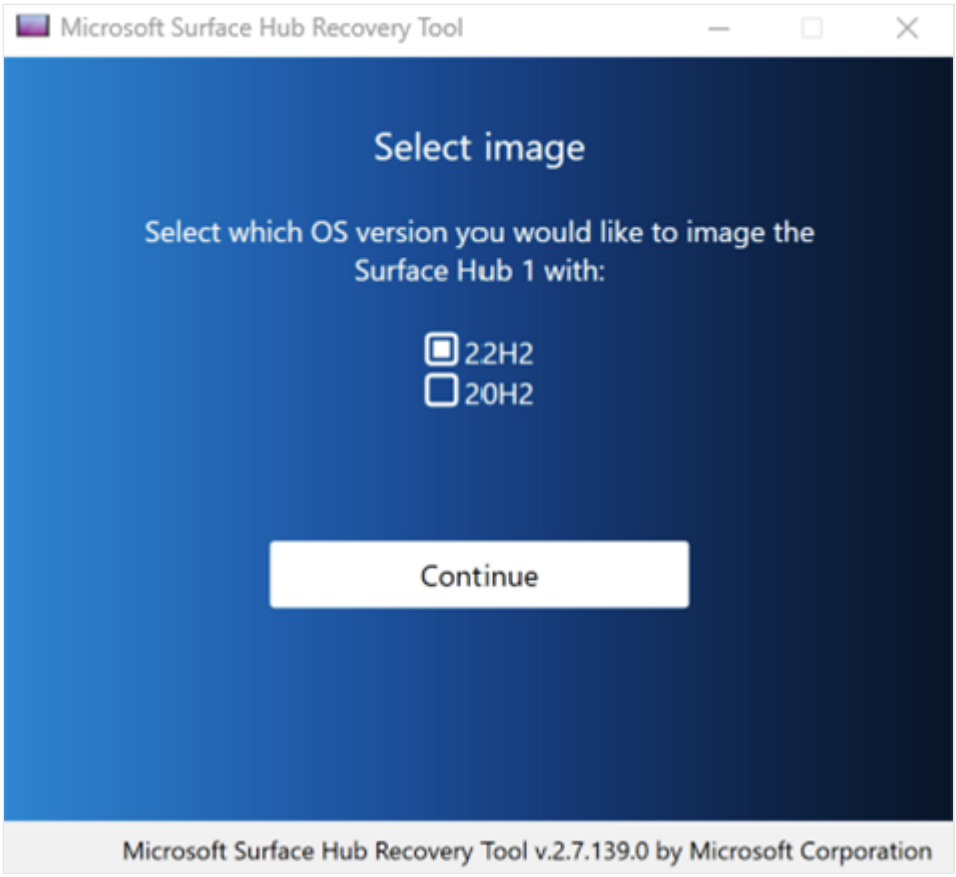
   

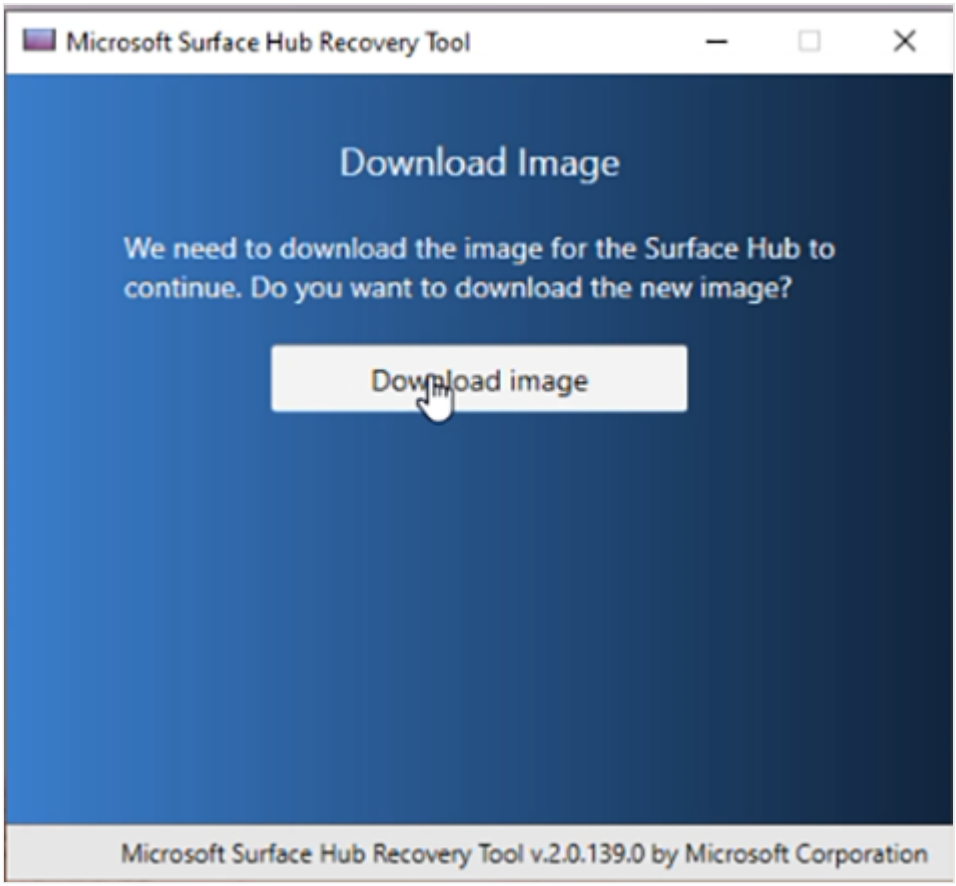
2. Select **Start**.

3. In the **Guidance** window, select **Next**.

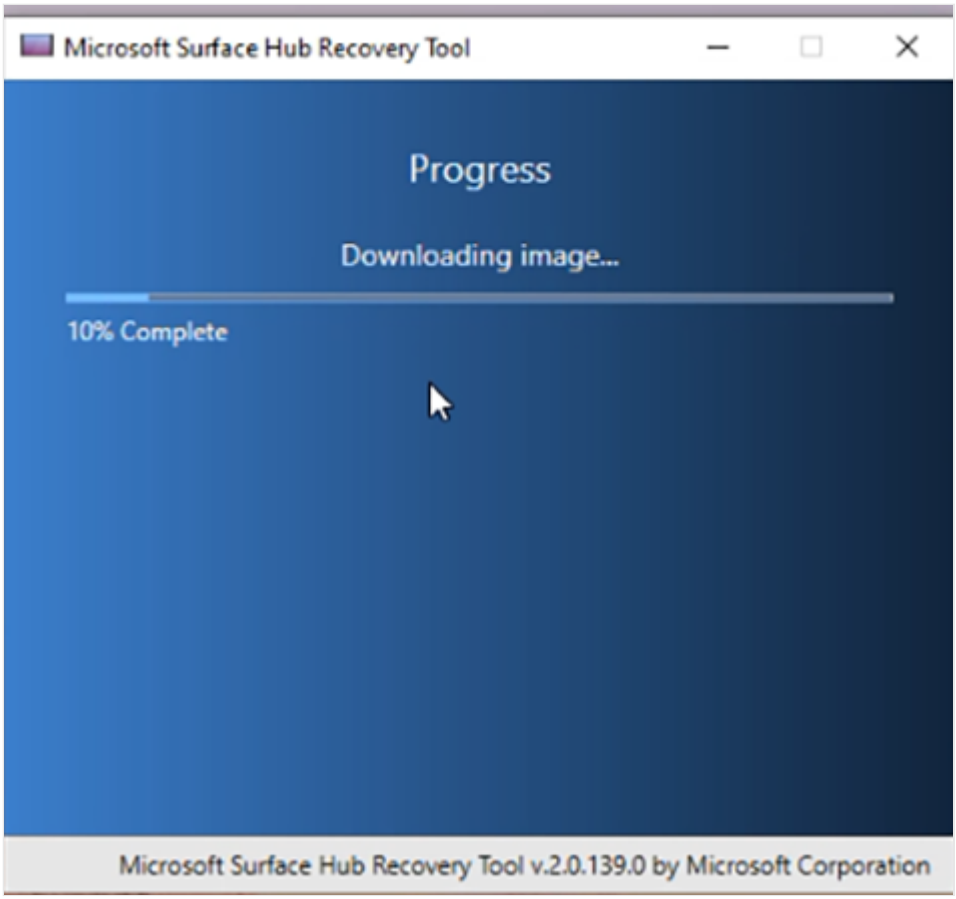


4. In the Select image window, select either **20H2** or its successor **22H2**, select **Continue,** and then select **Download image.**

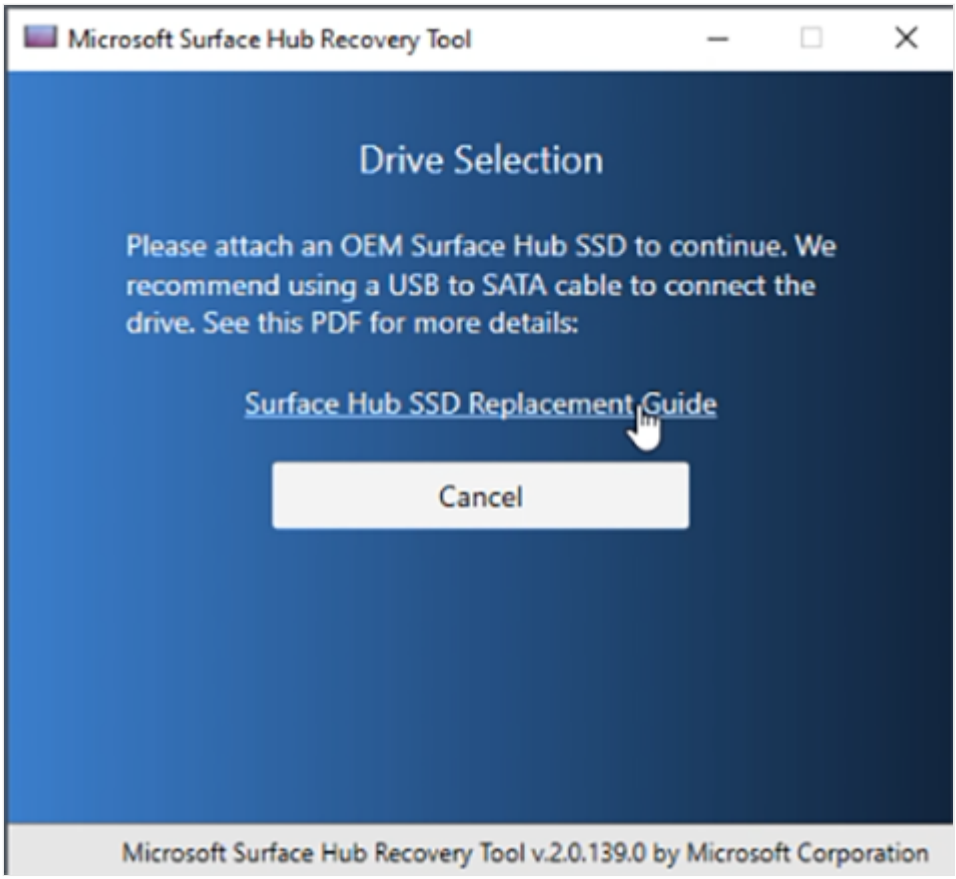




5. Time to download the recovery image is dependent on internet connection speeds. On an average corporate connection, it can take up to an hour to download the 8-GB image file.



6. When the download is complete, the tool instructs you to connect an SSD drive. If the tool is unable to locate the attached drive, there's a good chance that the cable being used isn't reporting the name of the SSD to Windows. The imaging tool must find the name of the drive as "LITEON L CH-128V2S USB Device" before it can continue. For more information on how to remove the existing drive from your Surface Hub, see Surface Hub SSD replacement.



7. When the drive is recognized, select **Start** to begin the reimaging process. On the warning that all data on the drive will be erased, select **OK**.

   Prior to applying the system image to the drive, the SSD is repartitioned and formatted. Copying the system binaries will take approximately 30 minutes, but can take longer depending on the speed of your USB bus, the cable being used, or antivirus software installed on your system.

Troubleshooting and common problems

Issue	Notes
The tool fails to image the SSD	Make sure you're using a factory-supplied SSD and one of the tested cables.
The reimaging process appears halted/frozen	It's safe to close and restart the Surface Hub Recovery Tool with no ill effect to the SSD.

Issue	Notes
The drive isn't recognized by the tool	Verify that the Surface Hub SSD is enumerated as a Lite-On drive, "LITEON L CH-128V2S USB Device". If the drive is recognized as another named device, your current cable isn't compatible. Try another cable or one of the tested cables listed on this page.
Error: -2147024809	Open Disk Manager and remove the partitions on the Surface Hub drive. Disconnect and reconnect the drive to the host machine. Restart the imaging tool again.

If the tool is unsuccessful in reimaging your drive, contact Surface Hub Support.

Version history

Version v2.7.139.0

This version of Surface Hub Recovery Tool adds support for Windows 10 Team 2022 Update (22H2).

Version v2.0.139.0

> **Important**
>
> This version is no longer functional. Please download the current version.

Use cloud recovery for BitLocker on Surface Hub

Article • 02/16/2023

This article describes how to use the cloud recovery function if you are unexpectedly prompted by BitLocker on a Surface Hub device.

> ⓘ **Note**
>
> You should follow these steps only if a BitLocker recovery key isn't available.

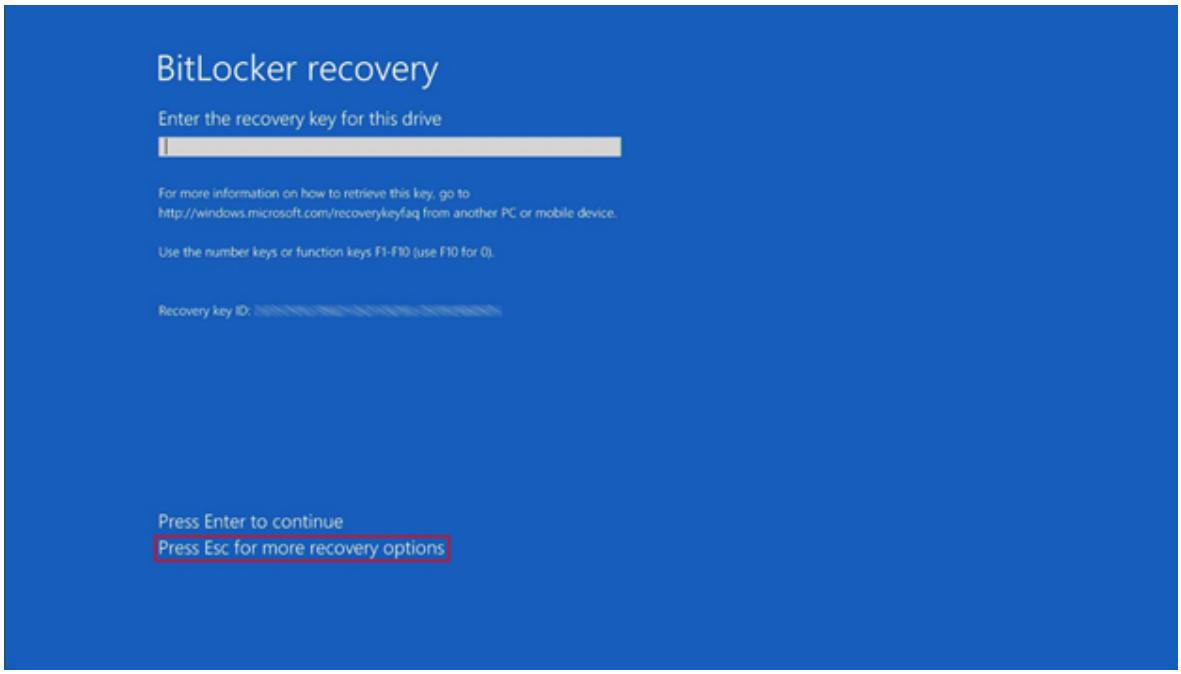
> ⚠ **Warning**
>
> - This recovery process deletes the contents of the internal drive. If the process fails, the internal drive will become completely unusable. If this occurs, you will have to log a service request with Microsoft for a resolution.
> - After the recovery process is complete, the device will be reset to the factory settings and returned to its Out of Box Experience state.
> - After the recovery, the Surface Hub must be completely reconfigured.

> ⓘ **Important**
>
> This process requires an open Internet connection that does not use a proxy or other authentication method.

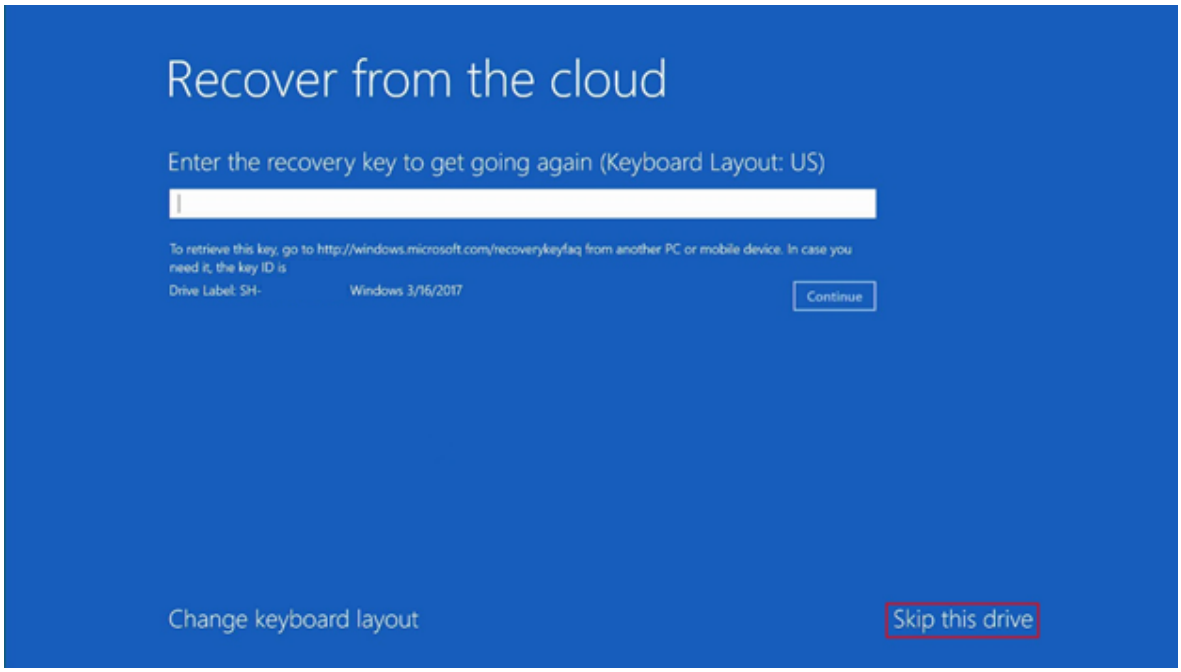
Cloud recovery process

To perform a cloud recovery, follow these steps:

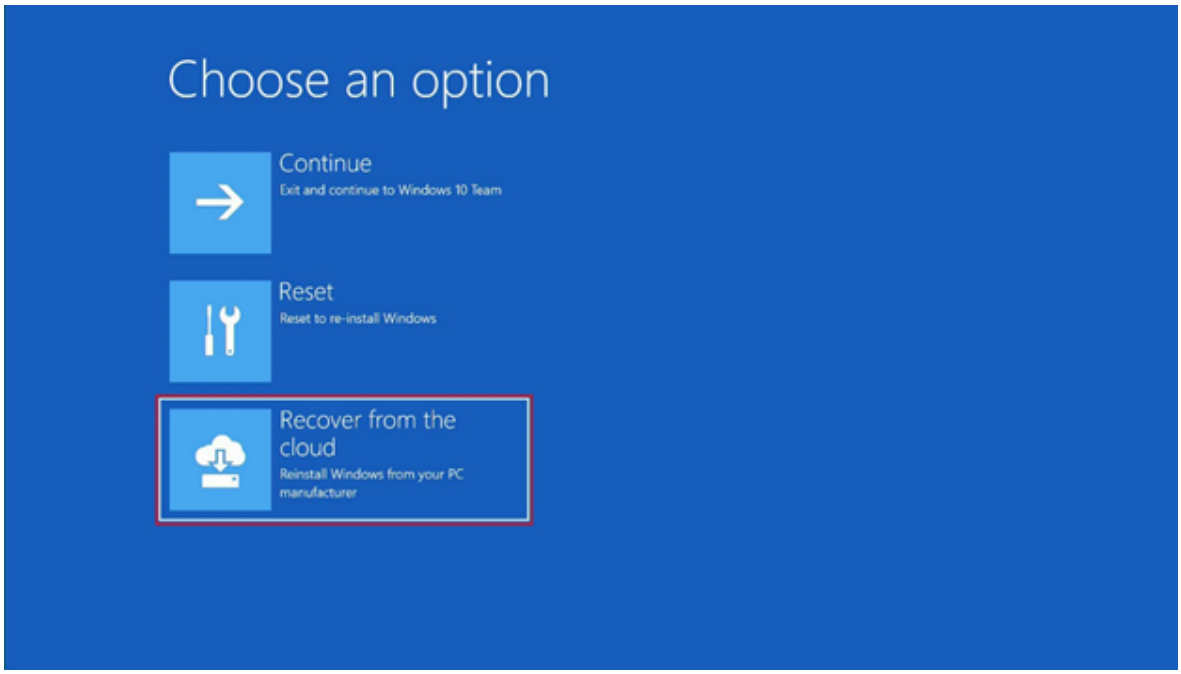
1. Select **Press Esc for more recovery options**.



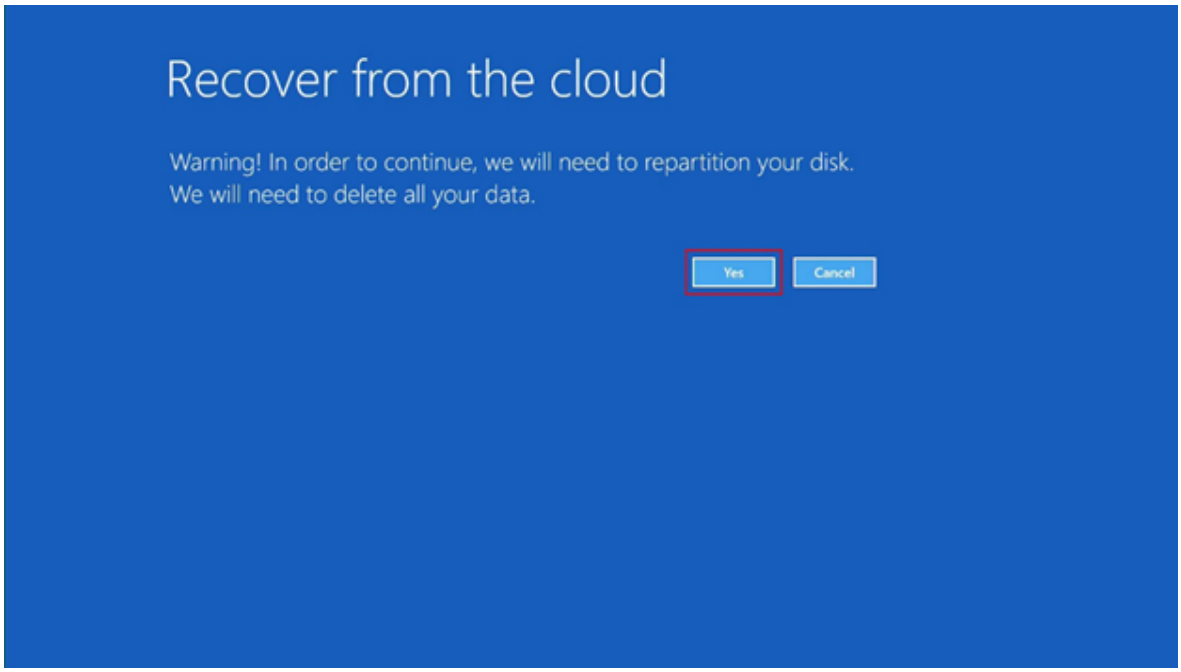
2. Select **Skip this drive**.



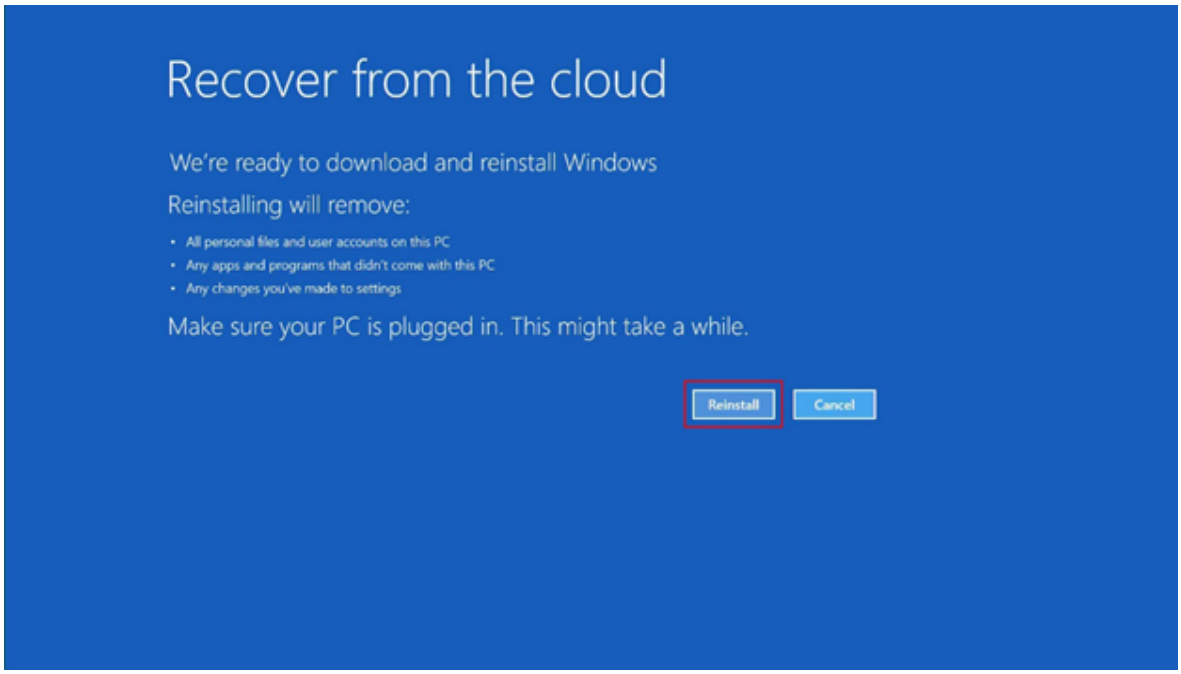
3. Select **Recover from the cloud**.

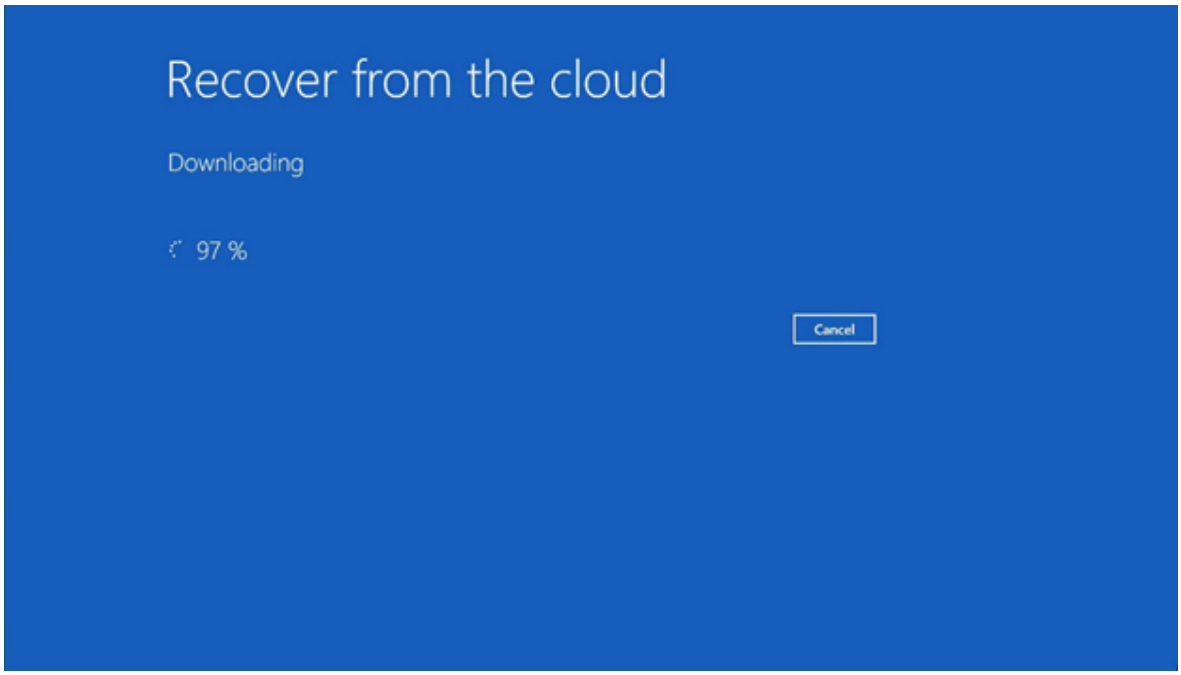


4. Select **Yes**.

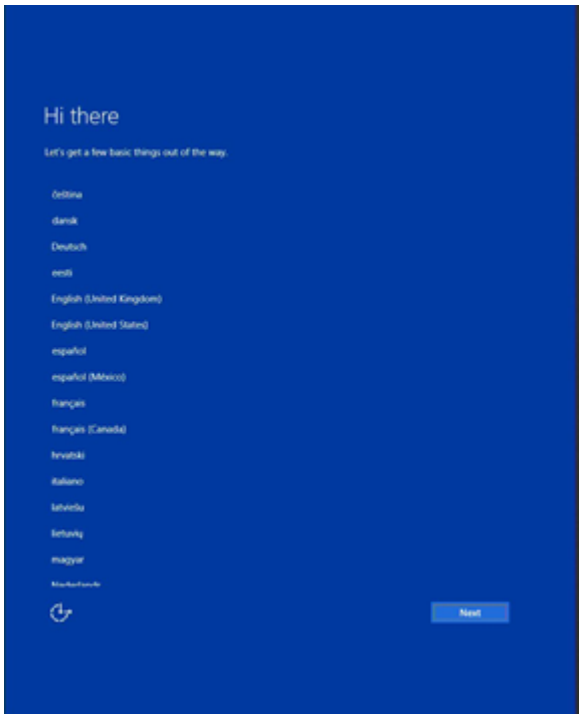


5. Select **Reinstall**.





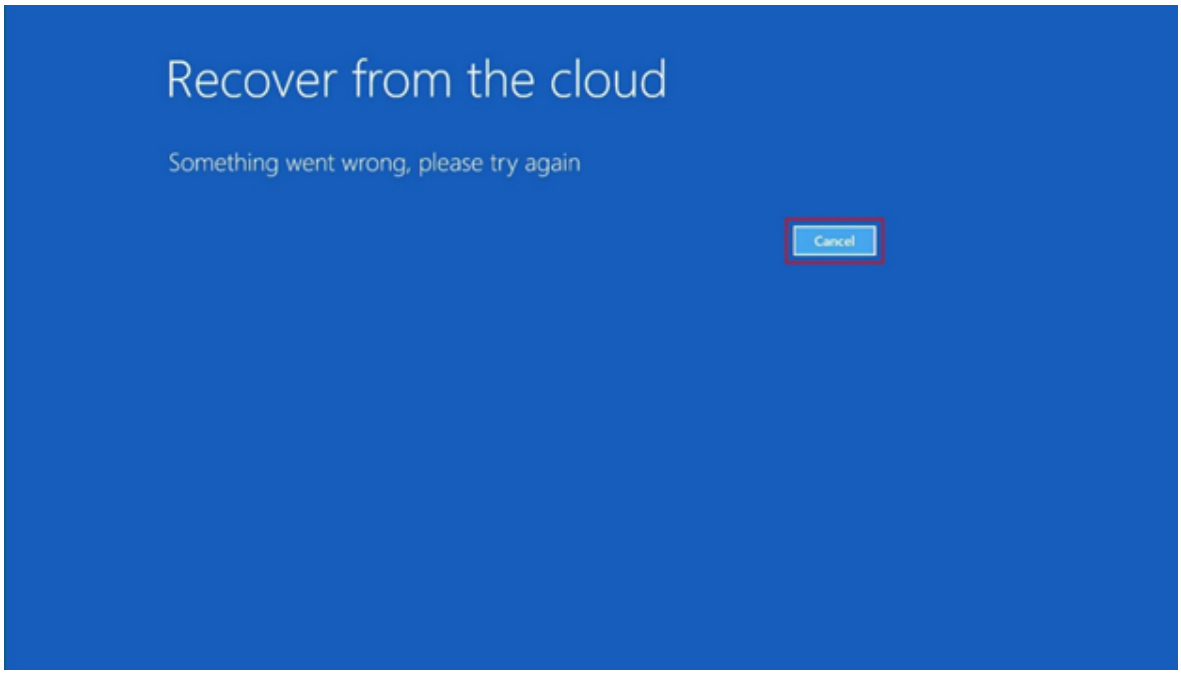
6. After the cloud recovery process is complete, start the reconfiguration by using the **Out of Box Experience**.



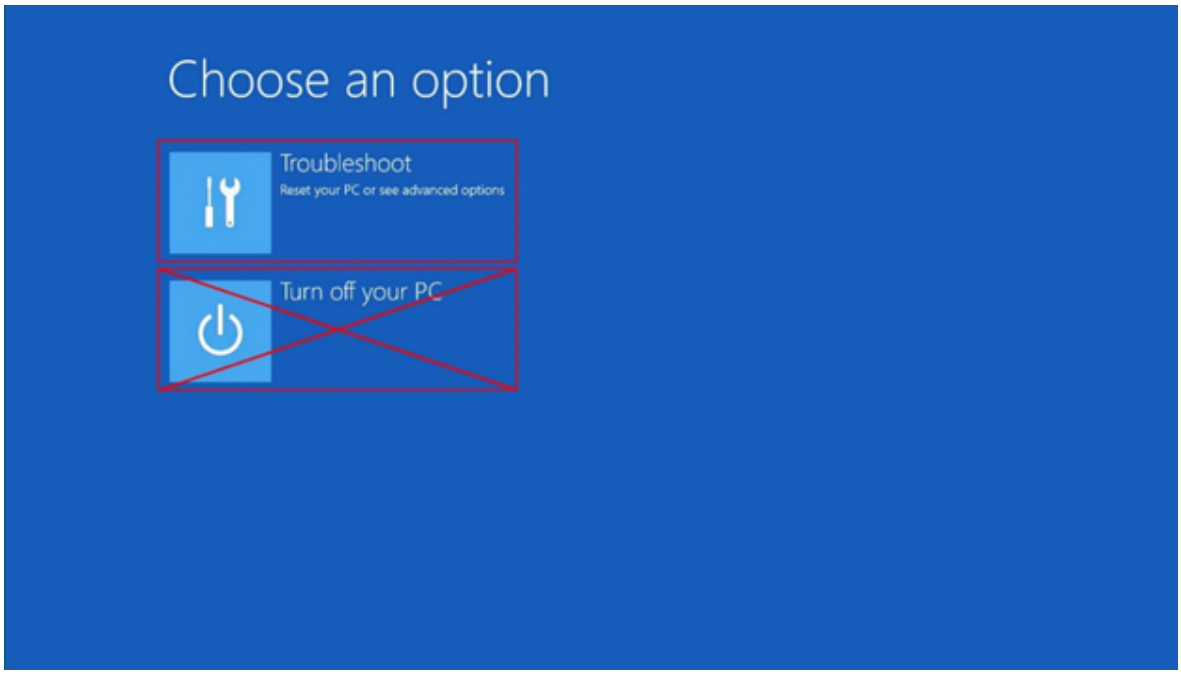
"Something went Wrong" error message

This error is usually caused by network issues that occur during the recovery download. When this issue occurs, don't turn off the Hub because you won't be able to restart it. If you receive this error message, return to the "Recover from the cloud" step, and then restart the recovery process.

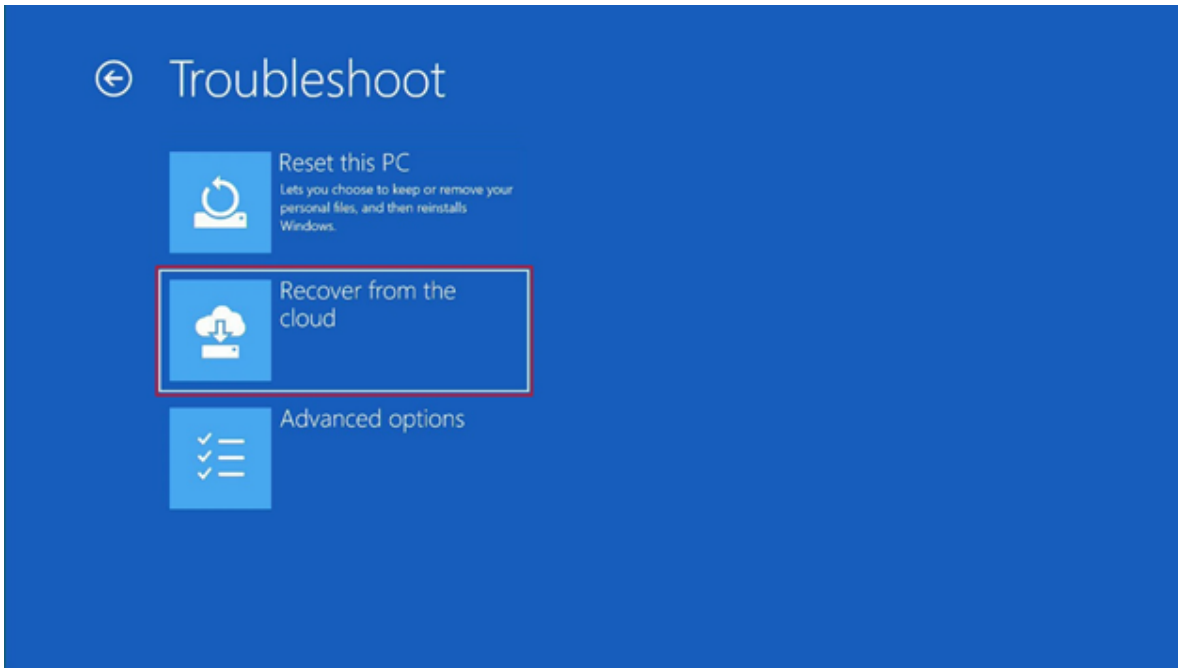
1. Select **Cancel**.



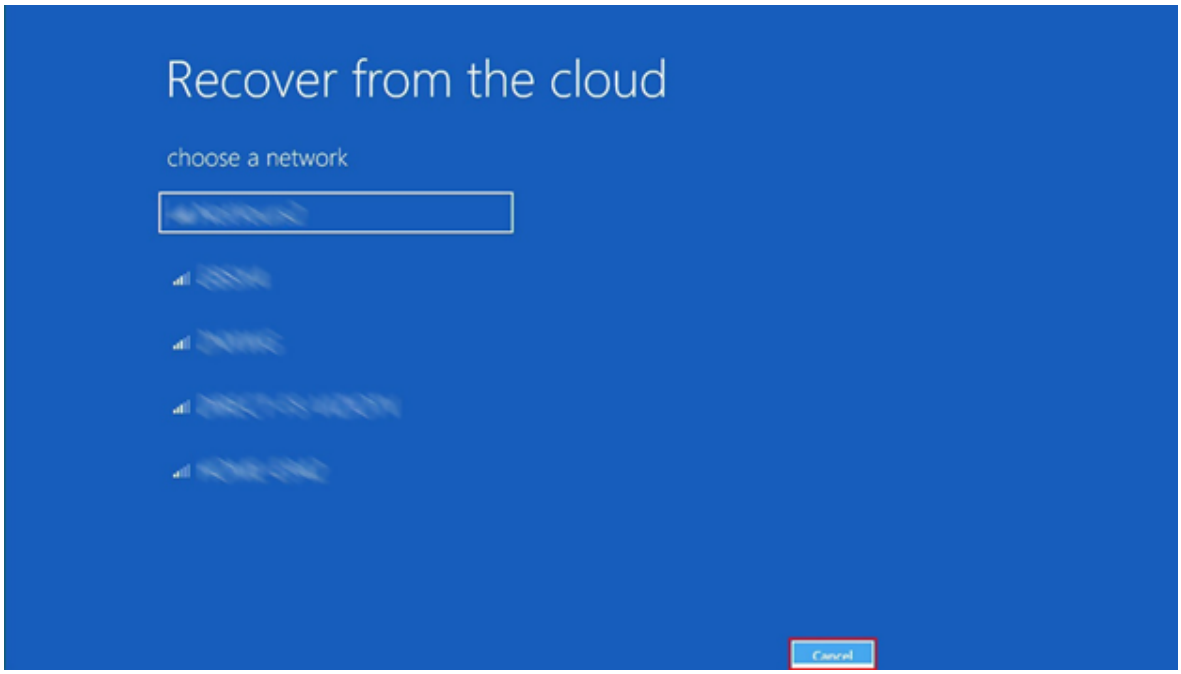
2. Select **Troubleshoot**.



3. Select **Recover from the cloud**.



4. If the **Wired network isn't found** error occurs, select **Cancel**, and then let the Surface Hub rediscover the wired network.


Recover from the cloud
choose a network
Cancel

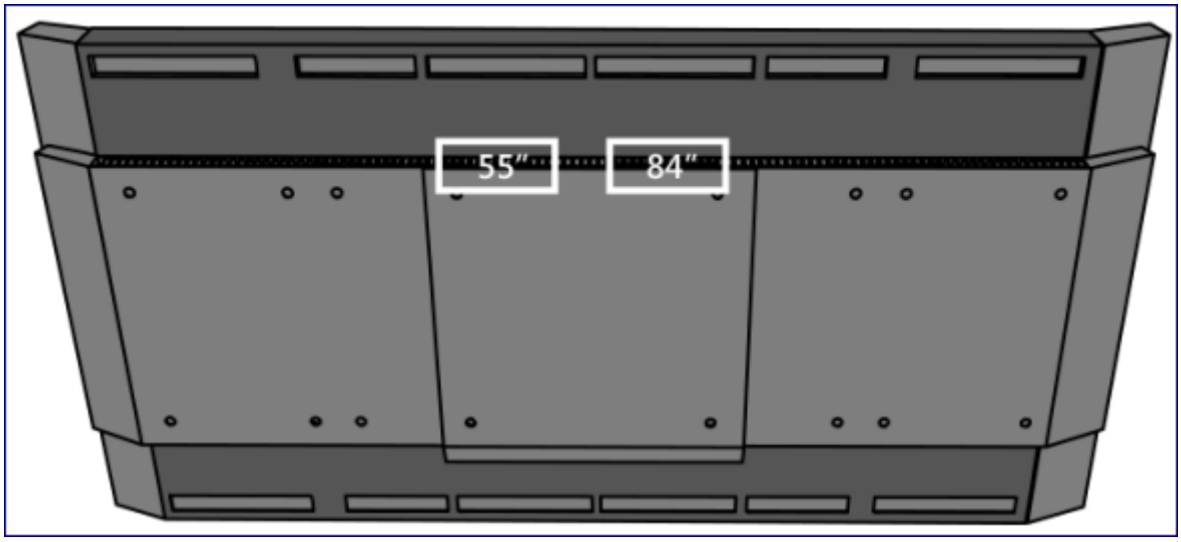
Surface Hub v1 SSD replacement

Article • 02/16/2023 • Applies to: Surface Hub v1

You might need to remove the solid state drive (SSD) from your Surface Hub so that you can reimage it using the Surface Hub Recovery Tool or because you've been sent a replacement drive. You would reimage your SSD when the operating system is no longer bootable, such as from a Windows update failure, BitLocker issues, reset failure, or hardware failure.

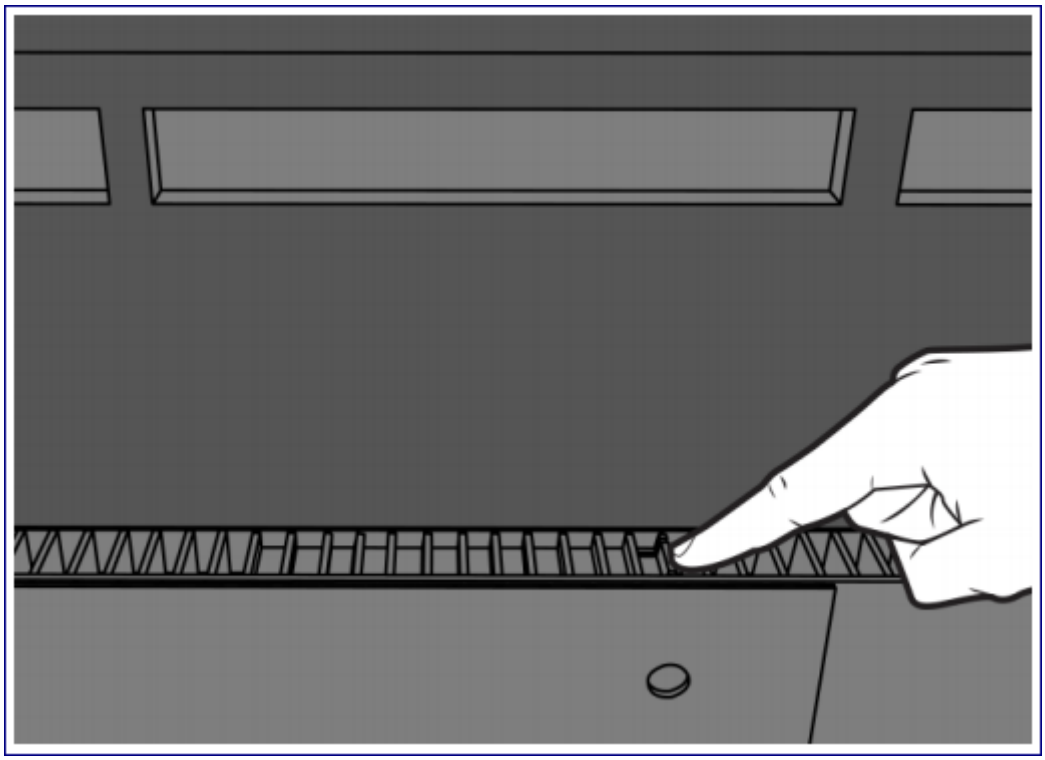
> ⚠ **Warning**
>
> Make sure the Surface Hub is turned off at the AC switch.

1. Locate the SSD compartment door on the rear, upper portion of the Surface Hub in the locations illustrated below. The door is identifiable as it doesn't have open ventilation slots.



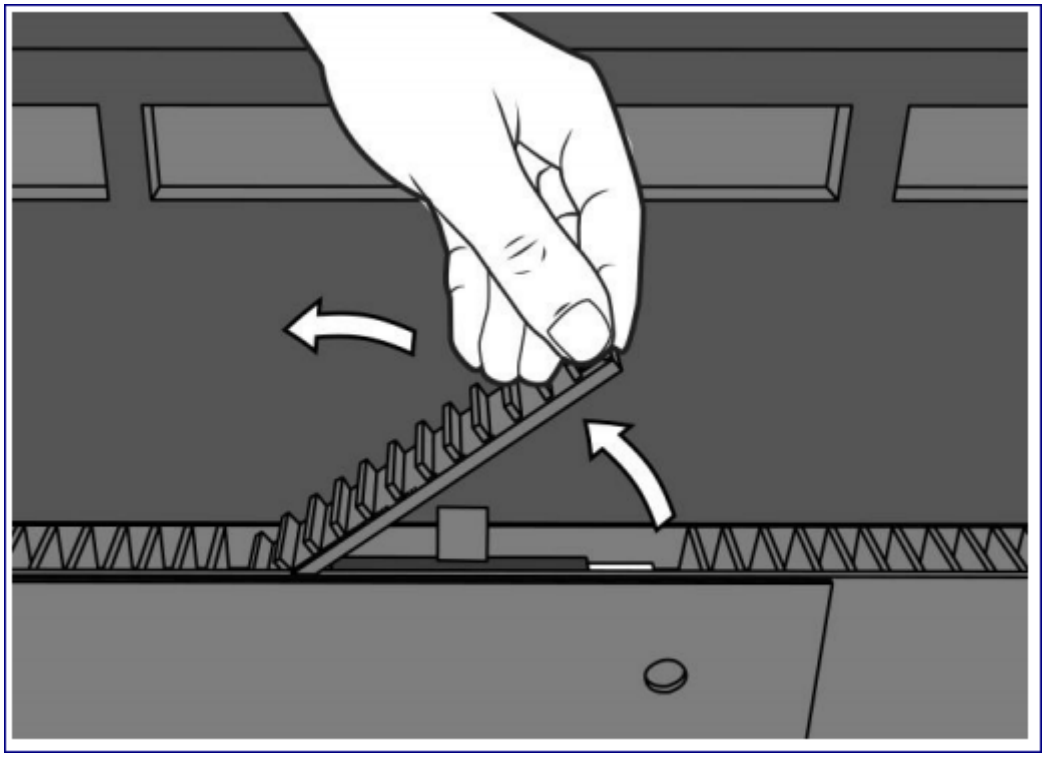
Surface Hub hard drive locations

2. Locate the locking tab on the hard drive compartment door. On the Surface Hub 55, the locking tab will be located on the left-hand side of the door. On the Surface Hub 84, it will be on the right-hand side as shown in the illustration.



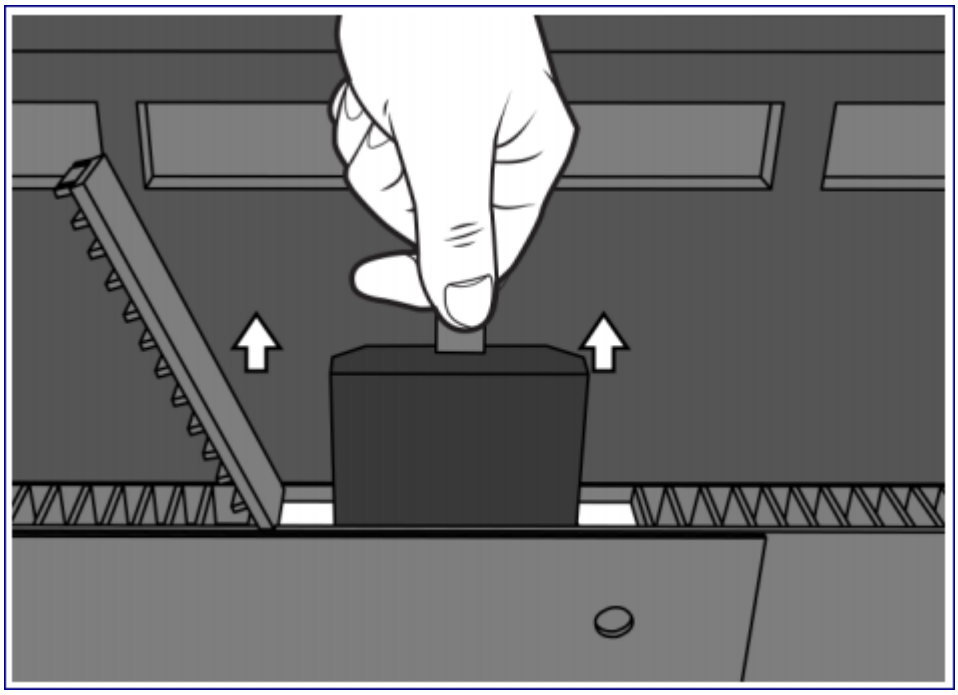
Locking tab on hard drive compartment door

3. Lift open the compartment door to access the hard drive.



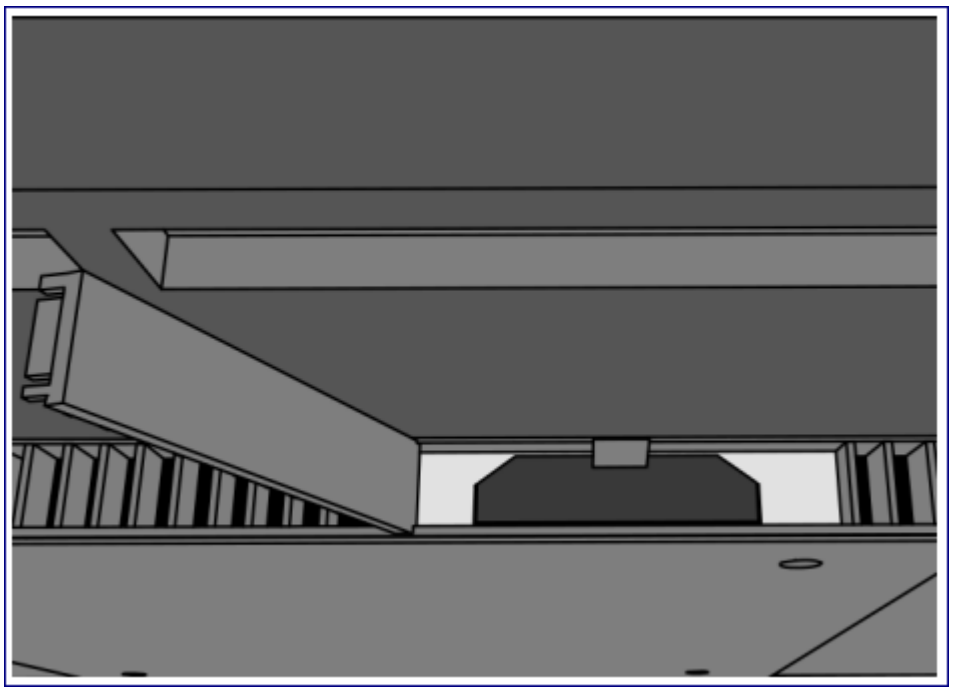
Lift compartment door

4. Locate the pull tab, which may be partially hidden under the rear cover. Pull on the tab to eject the hard drive from the compartment.



Pull tab

5. Slide the replacement drive into place until you hear it click.



Slide replacement drive into place

6. Close the compartment door.

7. Apply power to the Surface Hub.

Surface Hub Third-Party Stand Policy and Waiver

Article • 05/11/2023

This article provides Surface Hub Third-Party Stand Policy and Waiver for each country or region. To download the document, select the country or region where you purchased your Surface Hub.

To find other warranty terms in your country or region, go to Warranties, extended service plans, and Terms & Conditions for your device.

> **Note**
>
> To read the documents on this page, you must use a PDF viewer, PDF-enabled browser, or view through a device with PDF features enabled.

- Australia - English
- Belgique - Français
- België - Nederlands
- Canada - English
- Canada - Français
- Danmark - Dansk
- Deutschland - Deutsch
- España - Español
- France - Français
- Ireland - English
- Italia - Italiano
- Luxembourg - Deutsch
- Luxembourg - Français
- Malaysia - English
- Nederland - Nederlands
- New Zealand - English
- Norge - Bokmål
- Portugal - Português
- Qatar - English
- Schweiz - Deutsch
- Singapore - English
- Suisse - Français
- Suomi - Suomi

- Sverige - Svenska
- United Arab Emirates - English
- United Kingdom - English
- United States - English
- Österreich - Deutsch