Contents

- Reemplazo de SSD de Surface Hub
- Soluciones principales de soporte técnico para Surface Hub
- Solucionar problemas de Microsoft Surface Hub
- Problemas conocidos: sistema operativo Windows 10 Team
- Cómo usar la recuperación en la nube para BitLocker en un Surface Hub
- Uso de la herramienta de diagnóstico de hardware de Surface Hub para probar una cuenta del dispositivo
- Solucionar problemas de Miracast en Surface Hub
- Canales Miracast de Surface Hub 149-165 no admitidos en Europa, Japón ni Israel
- Qué hacer si la aplicación Connect de Surface Hub se cierra inesperadamente
- Surface Hub puede instalar actualizaciones y reiniciar fuera del horario de mantenimiento

Novedades de la actualización Windows 10 Team 2020

12/01/2022 • 4 minutes to read

Windows 10 Team 2020 Update ofrece mejoras importantes en la implementación y la facilidad de administración de dispositivos, junto con las características Windows 10 más recientes.

Implementación y facilidad de administración

- **Autenticación moderna para cuentas de dispositivo en la nube.** Surface Hub admite la autenticación basada en Exchange Web Services (EWS) y la biblioteca de autenticación de Active Directory (ADAL) para conectarse a Exchange, lo que permite a los clientes dejar de usar la autenticación básica. Para obtener más información, vea Modern authentication on Surface Hub.
- **Más de 20 configuraciones**de directiva de administración de dispositivos móviles (MDM) nuevas y actualizadas. Estas configuraciones de directiva dan a los administradores de TI un control mejorado sobre la configuración de varios dispositivos, incluidos: actualizaciones de aplicaciones de Microsoft Store, configuración de proyección inalámbrica como Miracast sobre infraestructura, configuración de red como calidad de servicio y autenticación por cable 802.1x y nueva configuración relacionada con la privacidad y el RGPD. Los nuevos proveedores de servicios de configuración (SPC) incluyen:
  - Cuentas de CSP
  - Firewall-CSP
  - RemoteWipe CSP
  - Wifi-CSP
  - Wirednetwork-CSP

Para obtener más información, vea:

- CSP admitidos en Microsoft Surface Hub
- Administrar Surface Hub con un proveedor MDM

Azure Active Directory Dispositivos unidos

- **Inicio de sesión único (SSO) para Azure AD dispositivos unidos.** Cuando los usuarios inician sesión con sus credenciales de Microsoft 365 en "Mis reuniones y archivos", sus credenciales de usuario fluyen sin problemas de una aplicación a otra, incluidas Microsoft 365 experiencias en el explorador.
- **Acceso condicional (CA) para Azure AD dispositivos unidos.** Los administradores de TI pueden controlar el acceso de los usuarios a los recursos de la organización Azure AD surface hubs unidos mediante la asignación de directivas de dispositivos de acuerdo con sus requisitos de seguridad y cumplimiento corporativos.
- **Compatibilidad con administradores no globales para Azure AD dispositivos unidos.** Los clientes pueden elegir un conjunto más detallado de administradores dentro de su jerarquía de administración para administrar Surface Hub. Para obtener más información, vea Configure non Global admin accounts on Surface Hub.

Explorador y lápiz

- **Nuevo Microsoft Edge instalado de forma predeterminada**. Microsoft Edge se ha reconstruido para

lograr un rendimiento de compatibilidad óptimo, seguridad y privacidad. Para obtener más información, vea Manage Microsoft Edge on Surface Hub.

- **Entrada de lápiz dual en Surface Hub 2S**. Los usuarios pueden hacer pizarras y colaborar en paralelo en Surface Hub 2S con dos Surface Hub 2 lápices. Las actualizaciones de firmware necesarias para habilitar la entrada de lápiz dual se liberarán con una actualización posterior.

Microsoft Teams

- **Microsoft Teams instalado de forma predeterminada**. Microsoft Teams se incluye como la aplicación predeterminada reuniones, llamadas y colaboración en nuevos dispositivos Surface Hub que se pueden cambiar o configurar a través de MDM o directamente en Surface Hub mediante la aplicación Configuración. Para obtener más información, vea [Deploy Microsoft Teams.

- **Compatibilidad con la unión de proximidad con Microsoft Teams**. Proximity Join permite a los usuarios realizar llamadas de Microsoft Teams programadas en un Surface Hub cercano con su portátil o teléfono, o bien realizar una transición sin problemas de una reunión en curso a un Surface Hub. Windows 10 Team actualización de 2020 agrega compatibilidad con administración de dispositivos móviles (MDM) para configurar la unión de proximidad. Para obtener más información, vea:

  - Microsoft Teams blog.
  - Administrar la configuración de Microsoft Teams en Surface Hub

- **Compatibilidad con reuniones coordinadas con Microsoft Teams**. En las salas de reuniones que cuentan con un Surface Hub y un dispositivo de sala de Microsoft Teams, o espacios con dos dispositivos Surface Hub, las reuniones coordinadas permiten a los usuarios aprovechar fácilmente ambos dispositivos durante una reunión Microsoft Teams. Con un solo toque, los usuarios pueden unirse a una reunión desde cualquier dispositivo y maximizar la propiedad de pantalla mostrando fuentes de vídeo en un dispositivo y una pizarra digital o contenido en el otro. Windows 10 Team 2020 Update agrega compatibilidad con administración de dispositivos móviles (MDM) para configurar reuniones coordinadas y la característica se lanzará posteriormente como una actualización Microsoft Teams a través de Microsoft Store. Para obtener más información, vea Set up Coordinated Meetings with Salas de Microsoft Teams and Surface Hub.

Seguridad

- **Inicio de sesión sin contraseña con claves de seguridad FIDO2** Con las claves de seguridad fido2, los clientes pueden iniciar sesión de forma rápida y Surface Hub sin tener que escribir nombres de usuario y contraseñas. Combinada con single Sign-On (SSO), esta característica proporciona una autenticación rápida y sin problemas a archivos, aplicaciones y sitios web durante una reunión. Para obtener más información, vea Configure passwordless sign-in on Surface Hub.
- **Mejoras en el inicio de sesión sin contraseña mediante Microsoft Authenticator**. Para las organizaciones que usan Azure AD, los usuarios pueden usar la aplicación Microsoft Authenticator para iniciar sesión sin tener que escribir nombres de usuario y contraseñas. Además, los usuarios pueden iniciar sesión con sus alias de correo electrónico preferidos en Azure AD además de su nombre principal de usuario (UPN). Para obtener más información, vea Sign in to Surface Hub with Microsoft Authenticator.

Obtén más información

- Windows 10 Team actualización 2020 1 publicada en todos los Surface Hub
- Instalar la actualización 2020 de Windows 10 Team

Especificaciones técnicas de Surface Hub 2S de 50 pulgadas

12/01/2022 • 2 minutes to read

ELEMENTO	DETALLES
Dimensiones	29,2" x 43,2" x 3,0" (741 mm x 1097 mm x 76 mm)
Dimensiones de envío	47,64" x 36,89" x 9,92" (1.210 mm x 937 mm x 252 mm)
Grosor	61,6 lb. (28 kg)
Peso del envío	81,08 lb. (36,77 kg)
Resolución	3840 x 2560
Pantalla	PixelSense Pantalla, relación de aspecto de 3:2, color de 10 bits, borde de 15,5 mm, deslumbramiento, PANTALLA IPS LCD
Procesador	Procesador Intel Core i5 de 8ª generación de cuatro núcleos, 8 GB de RAM, SSD de 128 GB [1]
Gráficos	Gráficos Intel UHD 620
Conexión inalámbrica	Wi-Fi 5 (compatible con IEEE 802.11 a/b/g/n/ac) Bluetooth tecnología Inalámbrica 4.1 Miracast pantalla
Conexiones	USB-A Mini-DisplayPort salida de vídeo 1.2 Ethernet DE 45 gigabits DE RJ (1000/100/10 BaseT) Entrada de vídeo HDMI (HDMI 2.0, HDCP 2.2 /1.4) USB-C con entrada DisplayPort Cuatro USB-C (en pantalla)
Sensores	Ocupación doppler [2] Acelerómetro Giroscopio
Audio/Vídeo	Altavoces estéreo de 3 vías de alcance completo y orientados frontalmente Matriz de micrófono MEMS de banda completa de 8 elementos Microsoft Surface Hub 2 cámara, 4K, conexión USB-C, 90 grados HFOV
Lápiz	Microsoft Surface Hub 2 bolígrafos (activo)

ELEMENTO	DETALLES
Software [3]	Windows 10 Microsoft Teams para Surface Hub Skype Empresarial Microsoft Whiteboard Microsoft Office (móvil) Microsoft Power BI
Exterior	Carcasa: aluminio mecado de precisión con resina compuesta por minerales Color: Platino Botones físicos: Power, Volume, Source
Qué hay en el cuadro	One Surface Hub 2S One Surface Hub 2 Pen Una Surface Hub 2 cámara Cable de alimentación de CA de 2,5 m Guía de inicio rápido
Garantía	Garantía limitada de hardware de 1 año [4]
BTU	1518 BTU/hr
Tensión de entrada	50/60Hz nominal de 110/230v, 90-265v max
Alimentación de entrada, en funcionamiento	445 W (carga de sobrecarga de 495 W)
Corriente de entrada	5.46 A
Energía de entrada, en espera	5 W max

NOTE

[1] El software del sistema usa un espacio de almacenamiento significativo. El almacenamiento disponible está sujeto a cambios en función de las actualizaciones de software del sistema y el uso de aplicaciones. 1 GB= 1.000 millones de bytes. Vea Surface.com/Storage para obtener más detalles.
[2] El sensor Doppler no está disponible en Hong Kong, India, Kuwait y Omán debido a las normativas locales.
[3] Licencia de software necesaria para algunas características. Se vende por separado.
[4] La garantía limitada de Microsoft se suma a los derechos de la ley del consumidor.

NOTE

Surface Hub puede usarse continuamente durante un máximo de 18 horas al día. Para optimizar la eficacia, Surface Hub usa sensores inteligentes para desactivar la pantalla LED cuando ya no se detecta la presencia, lo que significa que no es necesario apagarla al final del día. Si la unidad está instalada en un entorno de trabajo las 24 horas, los sensores se pueden deshabilitar para cumplir con la recomendación de uso máximo de 18 horas al día. Tenga en cuenta que la visualización prolongada de una señal de vídeo puede provocar que se produzca una grabación o retención de imágenes en la pantalla. Para obtener más información sobre cómo administrar la configuración de energía, consulte:

- Administración local para la configuración de Surface Hub
- CSP de SurfaceHub: administración Windows cliente

Surface Hub información general de 2S 85" & técnicas

12/01/2022 • 3 minutes to read

La versión de 85" de la familia Surface Hub ofrece la experiencia de Surface Hub 2S a espacios que requieren una pantalla más grande, como salas de conferencias, salas de reuniones o espacios de reunión más grandes. Surface Hub 2S 85" ofrece las siguientes experiencias:

- **Diseñado para la colaboración en grupo.** Invita a la entrada simultánea en Microsoft Whiteboard más asistentes remotos de mayor tamaño que la vida en Microsoft Teams.
- **Experiencia Surface Hub 2S coherente.** Proporciona el mismo diseño premium, tecnología de pantalla 4K, táctil, lápiz/tinta, cartucho de cálculo y compatibilidad con la cámara Surface Hub 2S 50".
- **Integración con sistemas A/V existentes y nuevos.** Se combina con Microsoft Teams periféricos certificados e se integra con Salas de Microsoft Teams.

Especificaciones técnicas de Surface Hub 2S 85"

COMPONENTE	DESCRIPCIÓN
Dimensiones	44,5" x 77,1" x 3,4" (1130 mm x 1959 mm x 85,6 mm)
Dimensiones de envío	89,5" x 62" x 22,8" (2275 mm x 1573 mm x 580 mm)
Grosor	185 lb (84 kg)
Peso del envío	399 lb (181 kg)
Resolución	3840 x 2160

COMPONENTE	DESCRIPCIÓN
Pantalla	PixelSense™ pantalla, relación de aspecto de 16:9, color de 10 bits, ancho de borde de 30,5 mm, antirrefecciones, IPS LCD, contacto en la celda con 20 puntos táctiles simultáneos
Cálculo	Modular Compute Cartridge Procesador Intel de 8ª generación de cuatro núcleos® core™ i5, 8 GB de RAM, SSD de 128 GB [1]
Software [2]	Windows 10 Team Sistema operativo Microsoft Teams para Surface Hub Skype Empresarial Microsoft Whiteboard Microsoft Office (móvil) Microsoft Power BI
Conexiones	USB-A Mini-DisplayPort salida de vídeo GIGABIT45 Gigabit Ethernet Entrada de vídeo HDMI USB-C® con entrada DisplayPort (3) USB-C® (en pantalla)
Gráficos	Intel® UHD Graphics 620
Audio y vídeo	100Hz: altavoces estéreo de 3 vías de intervalo de 12 KHz, incluidos (2) de rango medio/alto y (1) de rango medio/bajo en el protuberancia posterior. Matriz de micrófono MEMS de banda completa de 8 elementos Microsoft Surface Hub 2 cámara, 4K, conexión USB-C®, 90 grados HFOV
Lápiz	Microsoft Surface Hub 2 bolígrafos (activo) Compatible con lápiz de Surface Slim
Sensores	Sensor de ocupación Doppler [3]
Conexión inalámbrica	Wi-Fi 5: ieee 802.11 a/b/g/n/ac compatible Bluetooth® wireless 5.0 Miracast Mostrar
Exterior	Carcasa: aluminio mecado de precisión con resina compuesta por minerales Color: Platino Botones físicos: Power, Volume, Source
Qué hay en el cuadro	(1) Surface Hub 2S (2) Surface Hub 2 plumas (1) Surface Hub 2 cámara Cable de alimentación de CA de 4 m Guía de inicio rápido
Garantía	Garantía limitada de hardware de 1 año [4]
BTU	2047 BTU/hr

COMPONENTE	DESCRIPCIÓN
Tensión de entrada	50/60Hz nominal de 110/230v, 90-265v max
Alimentación de entrada, en funcionamiento	665 W (carga de sobrecarga de 745 W)
Corriente de entrada	7.8 A
Energía de entrada, en espera	5 W max

> **NOTE**
>
> Surface Hub puede usarse continuamente durante un máximo de 18 horas al día. Para optimizar la eficacia, Surface Hub usa sensores inteligentes para desactivar la pantalla LED cuando ya no se detecta la presencia, lo que significa que no es necesario apagarla al final del día. Si la unidad está instalada en un entorno de trabajo las 24 horas, los sensores se pueden deshabilitar para cumplir con la recomendación de uso máximo de 18 horas al día. Tenga en cuenta que la visualización prolongada de una señal de vídeo puede provocar que se produzca una grabación o retención de imágenes en la pantalla. Para obtener más información sobre cómo administrar la configuración de energía, consulte:
>
> - Administración local para la configuración de Surface Hub
> - CSP de SurfaceHub: administración Windows cliente

Referencias

1. El software del sistema y las actualizaciones usan un espacio de almacenamiento significativo. El almacenamiento disponible está sujeto a cambios en función del software del sistema y las actualizaciones y el uso de aplicaciones. 1 GB = 1.000 millones de bytes. 1 TB = 1.000 GB. Consulta Surface Storage para obtener más detalles.
2. Licencia de software necesaria para algunas características. Se vende por separado.
3. El sensor Doppler no está disponible en Hong Kong, India, Kuwait y Omán.
4. La garantía limitada de Microsoft se suma a los derechos de la ley del consumidor.

Obtén más información

- Surface Hub 2S 85": colaboración a escala masiva

Conceptos básicos del sistema operativo (Surface Hub)

12/01/2022 • 8 minutes to read

El sistema operativo de Surface Hub, Windows 10 Team, se basa en Windows 10 Enterprise y proporciona compatibilidad enriquecida para la administración empresarial, la seguridad y otras características. Sin embargo, hay importantes diferencias entre las dos versiones. Si bien la edición Enterprise está diseñada para equipos PC, Windows 10 Team está diseñado desde el principio para pantallas de gran tamaño y salas de reuniones. Al evaluar los requisitos de seguridad y administración de Surface Hub, es mejor considerarlo como un nuevo sistema operativo. Este artículo está diseñado para ayudar a destacar las diferencias clave entre Windows 10 Team en Surface Hub y Windows 10 Enterprise y qué significan las diferencias para las organizaciones.

A partir de septiembre de 2020, los clientes tienen la opción de migrar a Windows 10 Pro o Enterprise en Surface Hub 2S. Para conocer más, consulta lo siguiente:

- Anuncio de la disponibilidad de Windows 10 Pro y Enterprise en Surface Hub 2.
- Migrar a Windows 10 Pro o Enterprise en Surface Hub 2

Interfaz de usuario

Shell (interfaz de usuario del sistema operativo)

El shell de Surface Hub está diseñado desde el principio de modo optimizado para pantallas de gran tamaño y táctiles. No usa el mismo shell que Windows 10 Enterprise.

Directivas de la organización que esto puede afectar:

- La configuración relacionada con los controles el shell de Windows 10 Enterprise no se aplica s Surface Hub.

Protector de pantalla y pantalla de bloqueo

Surface Hub no tiene pantalla de bloqueo ni protector de pantalla, pero tiene una característica similar denominada la pantalla de inicio de sesión. La pantalla de inicio muestra las reuniones programadas el calendario de la cuenta del dispositivo y puntos de entrada fácil a las aplicaciones principales de Surface Hub - Skype Empresarial, la Pizarra interactiva y Conectar.

Directivas de la organización que esto puede afectar:

- La configuración de la pantalla de bloqueo, el tiempo de espera de pantalla y el protector de pantalla no se aplican a Surface Hub.

Inicio de sesión de usuario

Surface Hub está diseñado para usarse en espacios comunes, como las salas de reunión. A diferencia de los equipos con Windows, cualquier persona puede acercarse y usar Surface Hub sin iniciar sesión. Para habilitar esta funcionalidad común, Surface Hub no admite el inicio de sesión de Windows, mientras que Windows 10 Enterprise sí lo permite (por ejemplo, iniciar sesión con un usuario en el sistema operativo y usar esas credenciales en todo el sistema operativo). En su lugar, siempre hay un usuario local conectado automáticamente y con privilegios bajos que ha iniciado sesión en Surface Hub. No es compatible con el inicio de sesión de cualquier usuario adicional, incluyendo los usuarios administradores (por ejemplo, cuando un usuario administrador inicia sesión, no han iniciado sesión en el sistema operativo).

Los usuarios pueden iniciar sesión en Surface Hub, pero no iniciarán sesión en el sistema operativo. Por ejemplo, cuando un usuario inicia sesión en Aplicaciones o Mi reuniones y archivos, solo tiene acceso a las

aplicaciones o servicios, no al sistema operativo. Como resultado, el usuario que inició sesión es capaz de recuperar sus archivos y reuniones personales almacenadas de la nube, y estas credenciales se descartan al activar **Finalizar sesión**.

Directivas de la organización que esto puede afectar:

- Por lo general, Surface Hub usa características de bloqueo en lugar del control de acceso de usuario para aplicar la seguridad. Las directivas relacionadas con los requisitos de contraseña, el inicio de sesión interactivo, las cuentas de usuario y el control de acceso no se aplican a Surface Hub.

Guardar y explorar archivos

Los usuarios tienen acceso a un conjunto limitado de directorios en Surface Hub:

- Música
- Vídeos
- Documentos
- Imágenes
- Descargas

Los archivos que se guardan localmente en estos directorios se eliminan cuando los usuarios presionen **Terminar la sesión**. Para guardar contenido creado durante una reunión, los usuarios deben guardar los archivos en una unidad USB o en OneDrive.

Directivas de la organización que esto puede afectar: - Las directivas relacionadas con los permisos de acceso y la propiedad de archivos y carpetas no se aplican a Surface Hub. Los usuarios no pueden explorar ni guardar archivos en directorios del sistema ni carpetas de red.

Aplicaciones

Aplicaciones predeterminadas

Con pocas excepciones, las aplicaciones predeterminadas para la Plataforma universal de Windows (UWP) de Surface Hub también están disponibles en los equipos con Windows 10.

Aplicaciones para UWP instaladas previamente en Surface Hub:

- Alarmas y reloj
- Calculadora
- Conectar
- Excel Mobile
- Centro de opiniones
- Explorador de archivos
- Introducción
- Mapas
- Microsoft Edge
- Microsoft Power BI
- Microsoft Teams
- Microsoft Whiteboard
- OneDrive
- Fotos
- PowerPoint Mobile
- Configuración
- Tienda

- Sugerencias
- Word Mobile

Directivas de la organización que esto puede afectar:

- Usa las directrices de Windows 10 Enterprise para determinar las características y los requisitos de red de las aplicaciones predeterminadas en Surface Hub.

Instalar aplicaciones, controladores y servicios

Para ayudar a mantener la naturaleza del dispositivo, Surface Hub solo admite la instalación de aplicaciones para la Plataforma universal de Windows (UWP) y no admite la instalación de aplicaciones, servicios ni controladores clásicos de Win32. Asimismo, solo los administradores tienen acceso para instalar aplicaciones para UWP.

Directivas de la organización que esto puede afectar:

- Los empleados solo pueden usar las aplicaciones que hayan instalado los administradores, lo que ayuda a mitigar contra un uso no intencionado. Surface Hub no admite la instalación de los agentes de Win32 que la mayoría de las herramientas de administración y supervisión de PC tradicionales.

Seguridad y bloqueo

Para que Surface Hub se use en espacios comunes, como reuniones de las salas, su sistema operativo personalizado implementa muchas de las características de seguridad y bloqueo disponibles en Windows 10. Para obtener más información, vea Surface Hub de seguridad

Surface Hub implementa las siguientes características de seguridad de Windows 10:

- Arranque seguro
- Control de aplicaciones de Windows Defender y protección basada en la virtualización de la integridad del código
- Directivas de restricción de aplicaciones con AppLocker
- Cifrado de unidad BitLocker
- Módulo de plataforma segura (TPM)
- Antivirus de Microsoft Defender en Windows
- Control de cuentas de usuario (UAC) para acceder a la aplicación Configuración

Las siguientes características de Surface Hub proporcionan seguridad adicional:

- Firmware UEFI personalizado
- El shell y el menú Inicio personalizados limitan al dispositivo a las funciones de reunión
- El Explorador de archivos personalizado solo concede acceso a los archivos y las carpetas de Mis documentos
- La aplicación Configuración personalizada solo permite a los administradores modificar la configuración del dispositivo
- La descarga de controladores Plug and Play avanzados está deshabilitada

Directivas de la organización que esto puede afectar:

- Ten en cuenta las siguientes características al realizar la evaluación de seguridad de Surface Hub.

Administración

Configuración de dispositivo

Las opciones del dispositivo se pueden configurar a través de la aplicación Configuración. La aplicación

Configuración está personalizada para Surface Hub, pero también contiene muchas de las opciones de configuración familiares de Windows 10 Escritorio. Un mensaje de Control de cuentas de usuario (UAC) aparece en la pantalla cuando se abre la aplicación Configuración para comprobar las credenciales del administrador, pero este proceso no inicia la sesión del administrador.

Directivas de la organización que esto puede afectar:

- Los empleados pueden usar Surface Hub para reuniones, pero no pueden modificar las opciones de configuración del dispositivo. Además de las características de bloqueo, esto garantiza que los empleados solo usarán el dispositivo para las funciones de reunión.

Características de administración

Las características administrativas de Windows 10 Enterprise, como Microsoft Management Console, Ejecutar, Símbolo del sistema, PowerShell, Editor del registro, Visor de eventos y Administrador de tareas administrativas, no se admiten en Surface Hub. La aplicación Configuración contiene todas las características administrativas disponibles localmente en Surface Hub.

Administración y supervisión remotas

Surface Hub admite la administración remota a través de soluciones de administración de dispositivos móviles (MDM), como Microsoft Intune y supervisión a través de Azure Monitor.

Directivas de la organización que esto puede afectar:

- Surface Hub no admite la instalación de los agentes de Win32 que requiere la mayoría de las herramientas de administración y supervisión de equipos tradicionales, como System Center Operations Manager.

Directiva de grupo

Surface Hub no admite Windows de grupo, incluida la auditoría. En su lugar, usa MDM para aplicar directivas a Surface Hub. Para obtener más información sobre MDM, consulta Administrar la configuración con un proveedor de MDM (Surface Hub).

Directivas de la organización que esto puede afectar:

- Usa MDM para administrar Surface Hub en lugar de directivas de grupo.

Asistencia remota

Surface Hub no admite la asistencia remota.

Directivas de la organización que esto puede afectar:

- Las directivas relacionadas con la asistencia remota no se aplican a Surface Hub.

Red

Unirse a un dominio y unirse Azure Active Directory (Azure AD)

Surface Hub usa la unión a un dominio y la unión a Azure AD principalmente para proporcionar un grupo de administradores respaldados por el directorio. No se admite la combinación híbrida. Los usuarios no pueden iniciar sesión con una cuenta de dominio. Para obtener más información, consulta Administración del grupo de administradores.

Directivas de la organización que esto puede afectar:

- La configuración de directiva de grupo no se aplica cuando Surface Hub se une al dominio. La configuración de directiva relacionada con la pertenencia a un dominio no se aplica a Surface Hub.

Acceder a los recursos de dominio

Los usuarios pueden iniciar sesión en Microsoft Edge para acceder a sitios de intranet y recursos en línea (como Office 365). Si Surface Hub está configurado con una cuenta de dispositivo, el sistema la usa para acceder a

Exchange y Skype Empresarial. Sin embargo, Surface Hub no admite el acceso a recursos de dominio, como recursos compartidos de archivos e impresoras.

Directivas de la organización que esto puede afectar:

- Las directivas relacionadas con el acceso a objetos de dominio no se aplican a Surface Hub.

Datos de diagnóstico

El sistema de operativo de Surface Hub usa el componente Experiencia del usuario y telemetría asociadas de Windows 10 para recopilar y transmitir datos de diagnóstico. Para obtener más información, consulta Configurar los datos de diagnóstico de Windows en la organización.

Directivas de la organización que esto puede afectar:

- Configura los niveles de datos de diagnóstico de Surface Hub de la misma manera que lo harías para Windows 10 Enterprise.

Ajustar el brillo, el volumen y la entrada de Surface Hub 2S

12/01/2022 • 2 minutes to read

Surface Hub 2S proporciona una pantalla en pantalla para el volumen, el brillo y el control de entrada. El botón Origen funciona como una tecla de alternancia para cambiar entre los menús de control de volumen, brillo y entrada.

Para mostrar la pantalla en pantalla

- Mantenga presionado el **botón Origen** durante 4 segundos.

Cuando la pantalla en pantalla esté visible, use uno o más botones para alcanzar la configuración deseada.

Para ajustar el volumen

- Use el **botón Subir/bajar** volumen para aumentar o disminuir el volumen.

Para ajustar el brillo

1. Presione de **nuevo el botón** Origen para cambiar al menú de brillo.
2. Usa el **botón Subir/bajar** volumen para aumentar o disminuir el brillo.

Para ajustar la entrada

1. Presione el **botón Origen** dos veces para cambiar al menú Origen.
2. Usa el **botón Subir/bajar** volumen para cambiar entre entradas de PC, HDMI y USB-C.

Normativa general de privacidad de datos y Surface Hub

12/01/2022 • 2 minutes to read

En mayo de 2018, se aprobaba una ley de privacidad europea, el Reglamento general de protección de datos (RGPD). El RGPD impone nuevas reglas a las empresas, las agencias gubernamentales, las organizaciones sin ánimo de lucro y otras organizaciones que ofrecen bienes y servicios a personas de la Unión Europea (UE) o que recopilan y analizan datos vinculados a residentes de la UE.

Surface Hub clientes preocupados por la privacidad en virtud de las nuevas normativas del RGPD pueden administrar la privacidad de sus dispositivos con las siguientes opciones proporcionadas por Microsoft:

- **Opción 1: Surface Hub** dispositivos en regiones que se alocución en las regulaciones del RGPD reducen automáticamente la emisión de datos de diagnóstico a básico. Los clientes que opten por proporcionar un mayor nivel de datos de diagnóstico pueden usar la aplicación Surface Hub Configuración o la administración de dispositivos móviles para invalidar la configuración básica predeterminada.
- **Opción 2: Surface Hub** los clientes que desean quitar los datos de diagnóstico existentes pueden descargar la Surface Hub **eliminar** datos de diagnóstico desde el Microsoft Store. Esta aplicación permitirá a los clientes solicitar la eliminación de datos de diagnóstico asociados directamente desde Surface Hub dispositivo.

Microsoft tiene una amplia experiencia en la protección de datos, la protección de la privacidad y el cumplimiento de normativas complejas, y actualmente cumple con las cláusulas del Escudo de privacidad ue-EE. UU. y modelo de la UE. Creemos que el RGPD es un paso adelante importante para aclarar y habilitar los derechos de privacidad individuales. Queremos ayudarle a centrarse en su negocio principal a la vez que se prepara de forma eficaz para el RGPD.

Guía de preparación del sitio de Surface Hub 2S

12/01/2022 • 2 minutes to read

TEMA	DESCRIPCIÓN
Planificación de sitios para Surface Hub 2S	Revisar las consideraciones de sala y la planeación de periféricos.
Inicio rápido de Surface Hub 2S	Obtén información general sobre los pasos necesarios para desempaquetar e iniciar Surface Hub 2S.
Instalar y montar Surface Hub 2S	Obtén información sobre los accesorios con licencia para instalar y montar Surface Hub 2S.
Mover y controlar Surface Hub 2S 85"	Obtén información sobre cómo mover De forma segura Surface Hub 2S 85" a un espacio comercial.
Instalar y montar Surface Hub 2S 85"	Revisa las instrucciones recomendadas para instalar Surface Hub 2S 85".
Personalizar la instalación de Surface Hub 2S	Obtenga información sobre cómo personalizar la instalación sin accesorios de montaje con licencia.
Introducción a los puertos y el teclado numérico de Surface Hub 2S	Obtén información detallada sobre los puertos de E/S y los controles de selección y alimentación del teclado.
Conectarse a Surface Hub 2S	Obtén información sobre los métodos con cable e inalámbricos para conectarte a Surface Hub.

Planificación de sitios de Surface Hub 2S

12/01/2022 • 2 minutes to read

Introducción

Diseñado para la colaboración en equipo, Surface Hub 2S puede transformar su forma de trabajar: no solo en las salas de conferencias, sino en los lugares en los que desee trabajar. Una de las mayores ventajas de Surface Hub 2S es la posibilidad de moverla de un espacio a otro cuando se usa con el soporte móvil de Steelcase y la batería móvil. Con las funciones de trabajo en equipo desactivadas, Surface Hub 2S se puede integrar en casi cualquier área de trabajo.

Consideraciones sobre la sala

Diseñado para usarse de forma interactiva en salas de conferencia de menor tamaño y en espacios Huddle, Surface Hub 2S proporciona una cámara de 4K, matriz de micrófonos, altavoces nítidos y una pantalla brillante con una resolución de 4K. Optimizar la experiencia del usuario en espacios más grandes con más personas lejos de la pantalla puede requerir periféricos como cámaras, micrófono o solución para sistemas de salas adicionales, como salas de Microsoft Teams.

Como pauta general, instale Surface Hub 2S en un espacio que cumpla los siguientes criterios:

- Los usuarios pueden llegar a los cuatro bordes de la pantalla táctil.
- La pantalla no está en la luz solar directa, lo cual puede afectar a la visualización o dañar la pantalla.
- Las aberturas de ventilación no están bloqueadas.
- Los micrófonos no se ven afectados por las fuentes de ruido, como los ventiladores o los orificios de ventilación.
- El espacio está bien iluminado y no tiene orígenes reflectantes.

Ya sea que estén montados en una pared o instalados en el soporte móvil, las áreas donde usas el dispositivo deberían mantener:

- Las temperaturas de las salas no refrigerarán a 10 ° c (50 ° F) ni Hotter a 35 ° c (95).
- Humedad relativa no inferior al 20 por ciento ni superior al 80 por ciento.

Para obtener instrucciones detalladas sobre la planificación de la sala y más información sobre las salas de Microsoft Teams, consulte planear salas de Microsoft Teams.

Administración de la ubicación de Surface Hub 2S

Si tiene previsto usar Surface Hub 2S en un soporte móvil, es posible que desee explorar soluciones de terceros que habilitan los servicios de ubicación. Por ejemplo, los sistemas Active RFID pueden proporcionar seguimiento en tiempo real a través de espacios complejos de oficina o industriales. Para obtener más información, consulte con su proveedor de A/V o con otros conocimientos de terceros para obtener instrucciones.

Inicio rápido de Surface Hub 2S

12/01/2022 • 2 minutes to read

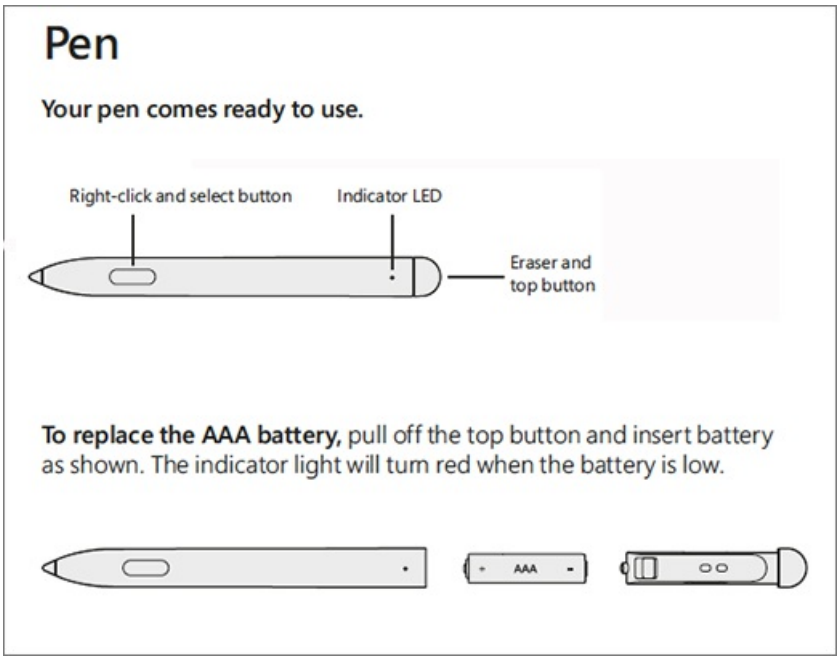
Desempaquetar Surface Hub 2S

1. Usa los controladores de cada lado del cuadro para moverlo al espacio donde lo configurarás.
2. Antes de abrir, quite los clips (4) de la parte frontal y posterior y, a continuación, levante la parte superior del cuadro con los controladores.
3. En la base de Surface Hub 2S, abra el cuadro de accesorios que contiene la guía de configuración, Surface Hub 2 lápiz, Surface Hub 2 cámara y el cable de alimentación.
4. En la parte posterior del Surface Hub, hay una etiqueta de instrucciones que muestra dónde adjuntar el hardware de montaje. Instáleslos en su lugar y quite la etiqueta.

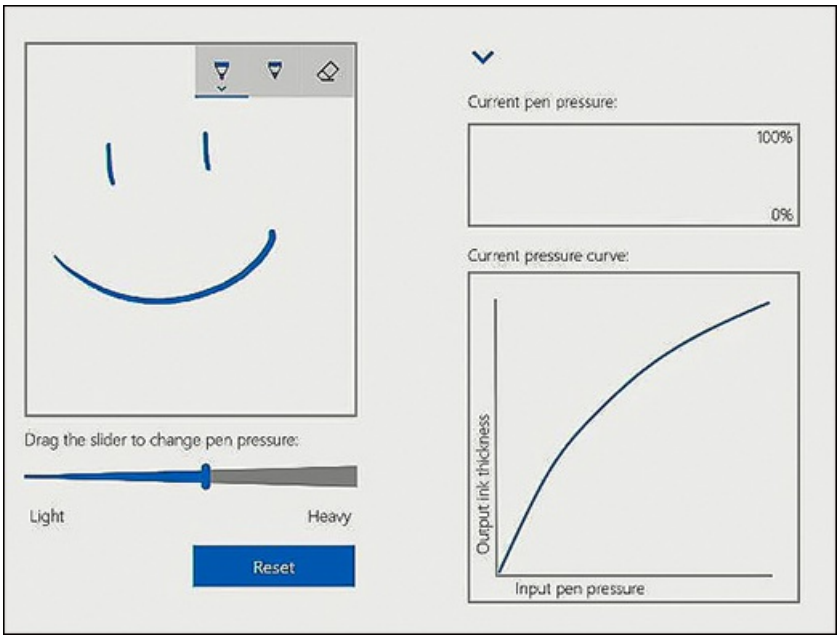
Vea este vídeo para obtener más información acerca de la desboxing y la configuración.

Instalar y ajustar el lápiz

1. Adjunte Surface Hub 2 plumas magnéticamente al lado preferido del dispositivo.



2. Para ajustar la presión del lápiz, abre la aplicación Surface en Surface Hub 2S, selecciona Lápiz y ajusta el control deslizante.



Instalar cámara

Quite la lente de la cámara y adjuntela al puerto USB-C en la parte superior del Surface Hub 2S.

Iniciar Surface Hub 2S

1. Inserte el cable de alimentación en la parte posterior del dispositivo y conéctelo a una toma de corriente. Ejecute el cable a través de las guías de cable de la solución de montaje y quite el panel de pantalla.
2. Para empezar, presione el botón de encendido en la parte inferior derecha.

Instalar y montar Surface Hub 2S 50"

12/01/2022 • 2 minutes to read

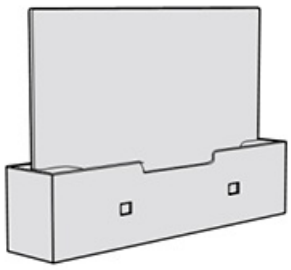
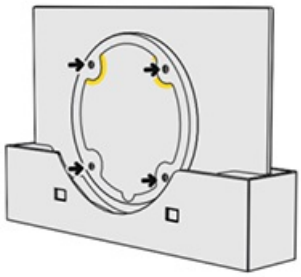
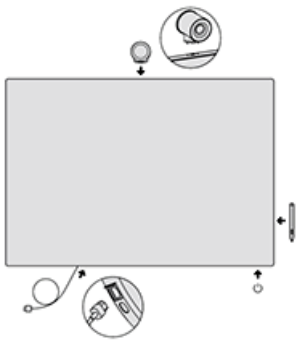
Surface Hub 2S 50" está diseñado para facilitar la movilidad con un factor de forma que te permite instalar rápidamente y empezar a usar el dispositivo. Microsoft se ha asociado con Steelcase en las siguientes soluciones de montaje certificadas: Roam Mobile Stand y Roam Wall Mount. Ambos se integran completamente con el diseño de Surface Hub 2S 50", lo que permite un acceso sin intervención al cartucho de cálculo, la alimentación, USB-A, USB-C y otros puertos.

Puede montar Surface Hub 2S 50" con el soporte de pared certificado o el soporte móvil certificado, ambos desarrollados en asociación con Steelcase. Ambos se integran completamente con el diseño de Surface Hub 2S 50", lo que permite un acceso sin intervención al cartucho de cálculo junto con todos los puertos de E/S y la alimentación.

Para obtener más información, consulta Accesorios de terceros con licencia oficial y ver las demostraciones de instalación del equipo de producto de Surface en el stand móvil de Steelcase y la batería de APC configurada.

Si no usa accesorios con licencia, vea Personalizar montaje en pared de Surface Hub 2S 50".

1. CONFIGURE EL MONTAJE PRIMERO	

1. CONFIGURE EL MONTAJE PRIMERO	
Deje el Surface Hub en el cuadro hasta que se configure el montaje y se aplique el hardware de montaje. El montaje no está incluido. El montaje se vende por separado.	
2. **Adjunte hardware al Surface Hub**	
El hardware de montaje y las instrucciones específicas se encuentran en la caja del montaje.	
3. **Quite la etiqueta de instrucciones antes de montarla.**	
Obtén a alguien que te ayude a levantar y montar tu Surface Hub. Asegúrese de mantener y levantar el Surface Hub desde la parte inferior.	
4. **Conecte los accesorios y la alimentación**	
Instale los accesorios y adjunte el cable de alimentación como se muestra. Consulta guías en la pantalla. Quite el ajuste de ajuste de la pantalla. Presione el botón de encendido para encender.	

Mover y controlar Surface Hub 2S 85"

12/01/2022 • 2 minutes to read

Para obtener instrucciones prácticas recomendadas sobre cómo mover Surface Hub 2S 85, consulta:

- Instalar y montar Surface Hub 2S 85"

Más información

- Un vistazo en profundidad al nuevo Surface Hub 2S 85"

Instalar y montar Surface Hub 2S 85"

12/01/2022 • 8 minutes to read

En este artículo se proporcionan instrucciones de soporte técnico para instalar físicamente Microsoft Surface Hub 2S 85" en entornos comerciales.

Vídeo de desboxing

- Antes de comenzar, revise Microsoft Surface Hub vídeo de 2S 85" Unboxing and Set Up:

Seguir todas las precauciones de seguridad

WARNING

Administración y preparación del sitio

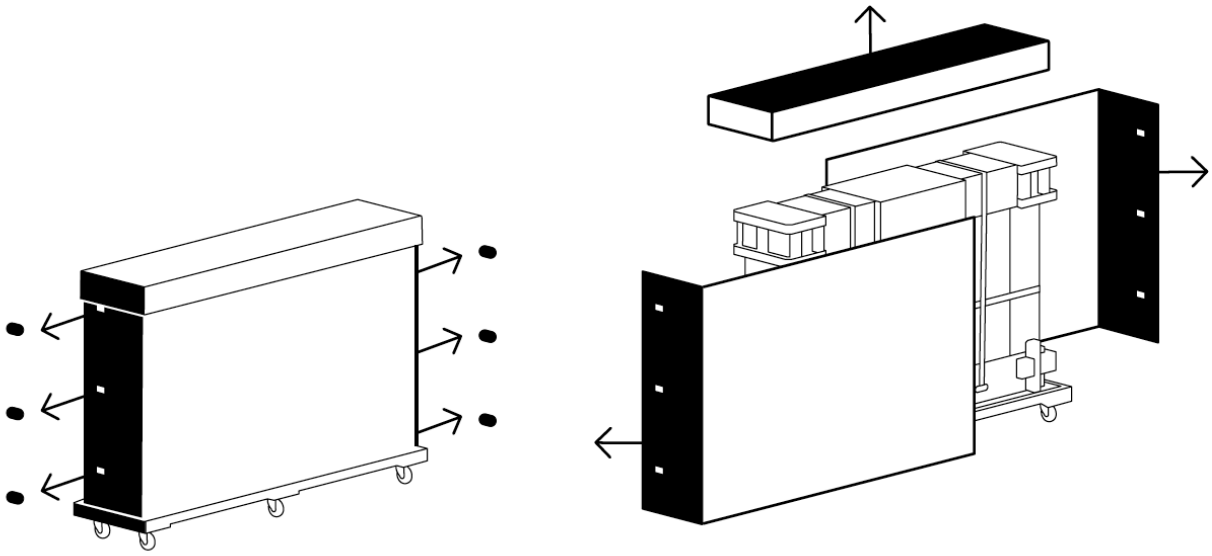
- El dispositivo es muy pesado. Para reducir el riesgo de daños personales, muerte o daños en el dispositivo debido a su tamaño y peso, es importante mantener el dispositivo vertical.
- Antes de mover el dispositivo al lugar donde se instalará, consulte el sitio para determinar cómo moverlo de forma segura a la ubicación donde se desempaquetará y montará.
- Use siempre al menos dos personas para desempaquetar e instalar.
- Una vez que el dispositivo se desempaquete, debe montarse inmediatamente, por lo que el sistema de montaje debe estar en su lugar antes de desempaquetar. Si vas a montar en un soporte enrollable, bloquea o bloquea las ruedas del soporte antes de desempaquetar.
- Para evitar riesgos de tropiez, mantenga el área de ensamblado libre de materiales de empaquetado.

IMPORTANT

Antes de continuar, revise la información de seguridad adicional que se muestra a continuación en el Apéndice A.

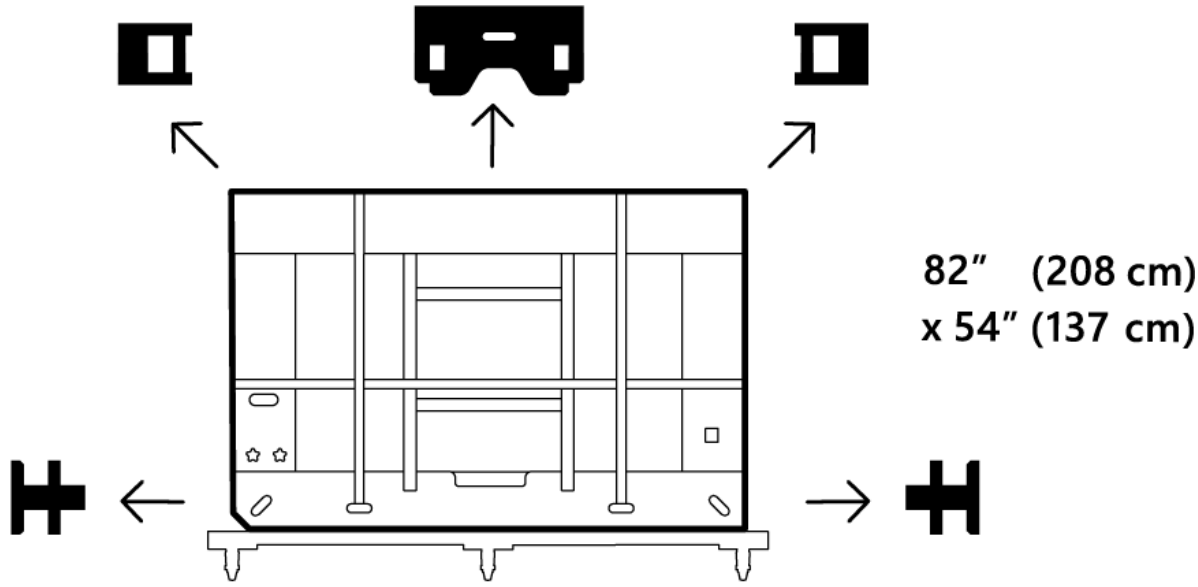
1. Quitar los materiales de empaquetado externos

1. Quitar y reciclar la cubierta externa.
2. Corte cuatro (4) correas de plástico.
3. Abra y quite los seis (6) clips de los extremos.
4. Quite la tapa y, a continuación, levante y quite los paneles frontal y posterior.



2. Quitar la espuma de empaquetado exterior negro

1. Quite las piezas de espuma de esquina negra (4).
2. Quite el soporte de la espuma central negra.

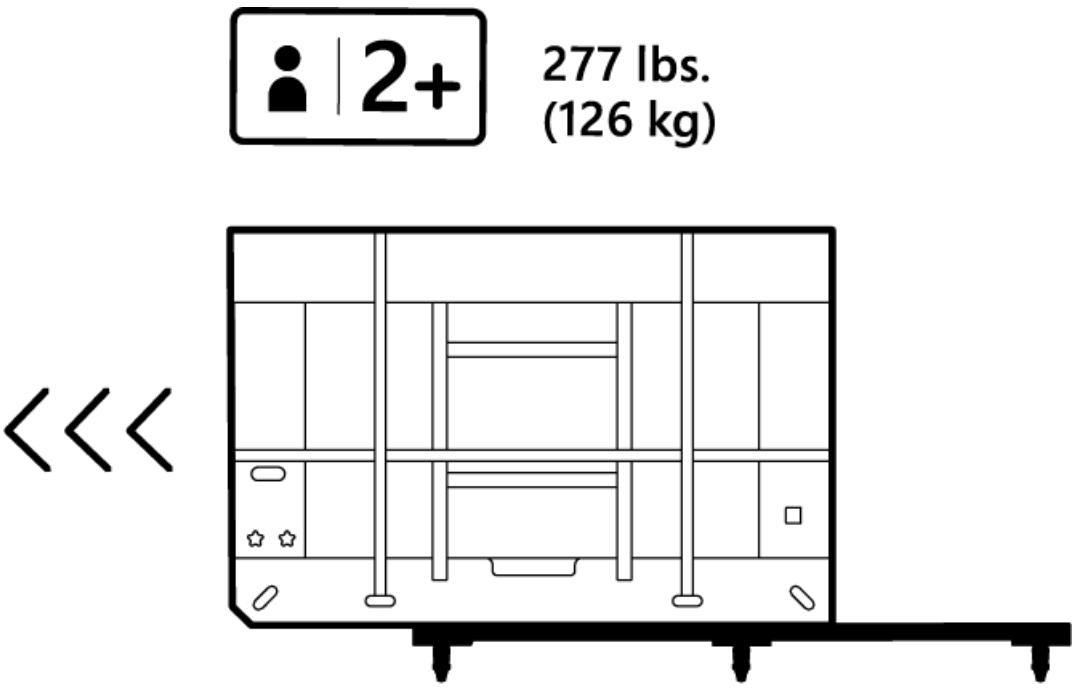


Caution

No quite la espuma blanca, los flejes ni los materiales de empaquetado hasta que hub 2S esté adyacente al carro o montaje en la pared en el que se colocará. Los materiales de fleje adicionales se proporcionan en la pequeña caja situada debajo de los botones del lado posterior del paquete. Los materiales de fleje originales o de reemplazo deben estar en su lugar antes de moverse y, especialmente, antes de girar el dispositivo y su paquete de protección

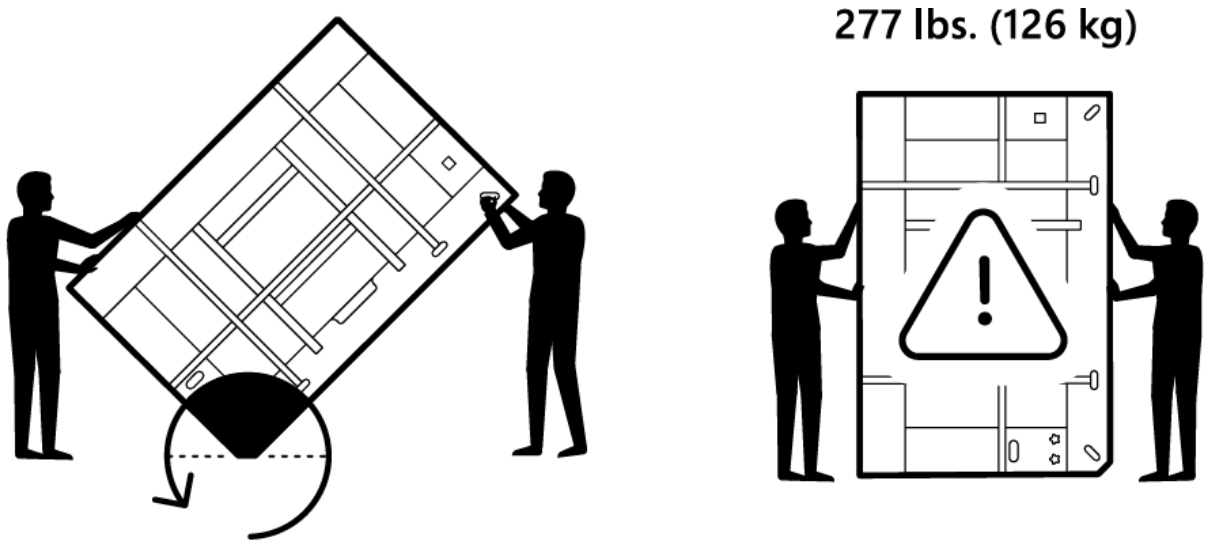
3. Quitar el marco de empaquetado interno de la paleta

1. Mueva el ensamblado de paletas a la ubicación del elevador.
2. Frenos de rueda de bloqueo (4).
3. Deslice el empaquetado interno fuera de la paleta.



4. Girar el marco de empaquetado para ajustarse al elevador

1. Girar marco para ajustarse al elevador
2. Gira en el extremo biselado del marco interior y desliza hacia el elevador.

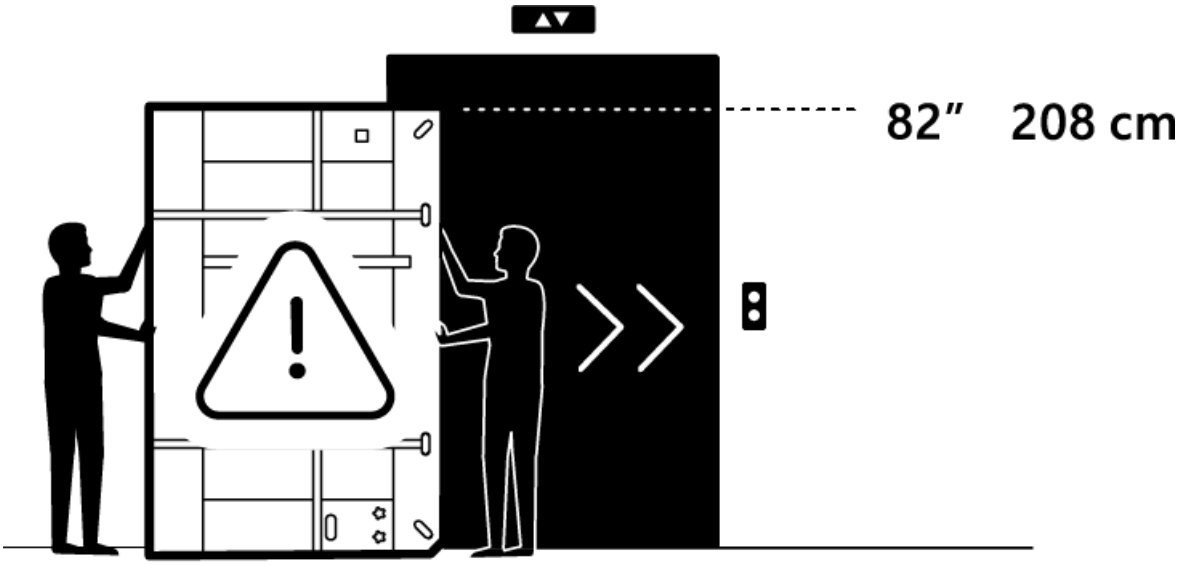


TIP

La paleta con rueda se ajusta de forma personalizada a la superficie de empaquetado del marco interno y se puede usar durante todo el proceso de entrega del sitio de instalación. La parte final del marco de madera interna tiene planchas de cinta de nilón.

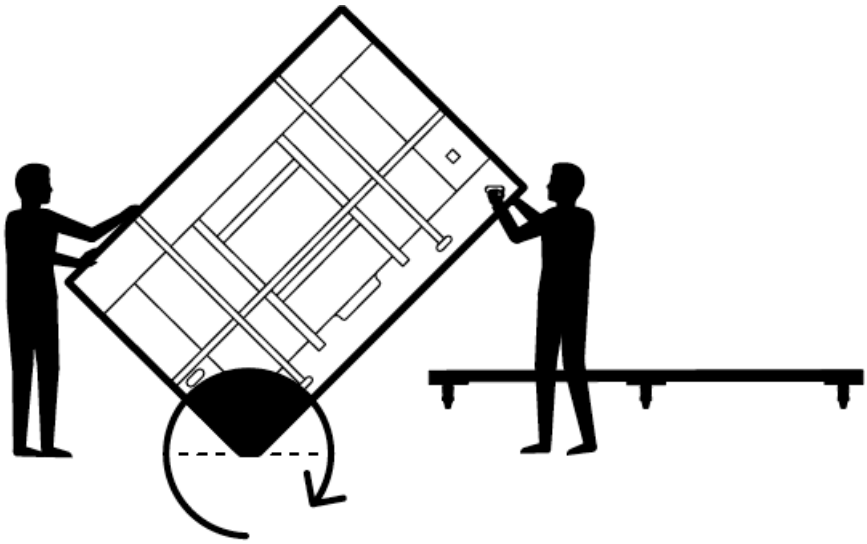
5. Quitar del elevador

1. Deslizarse fuera del elevador
2. Frenos de rueda de bloqueo (x4).



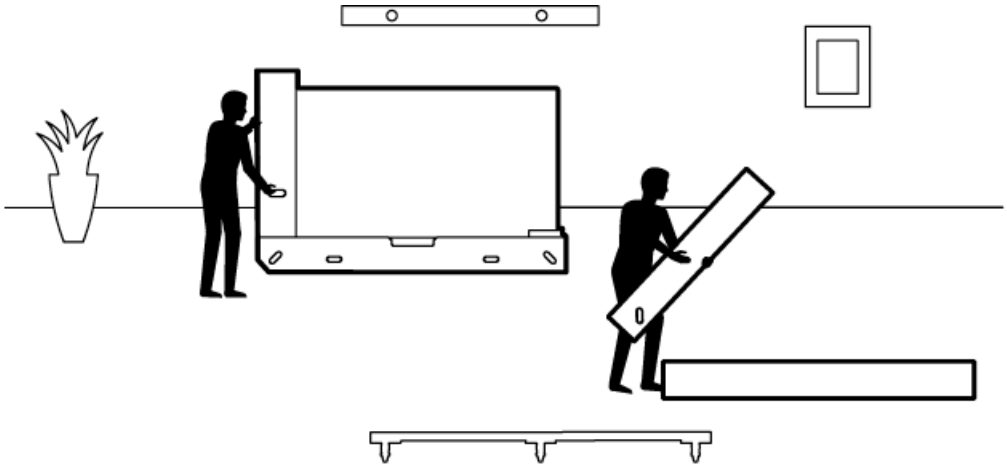
6. Vuelva Surface Hub 85" en la paleta

1. Con el extremo biselado, gira hacia atrás sobre la paleta.
2. Desbloquear frenos de rueda (x4).
3. Mueva el producto a la ubicación del montaje de la pared o del carro.



7. Coloque Surface Hub 85" en el montaje en pared o en el carro

1. Coloque el concentrador 2S delante de la pared o del carro.
2. Frenos de rueda de bloqueo (x4).
3. Deslice el empaquetado interno fuera de la paleta.
4. Corte las 3 correas de plástico.
5. Quite la tapa.
6. Quite las piezas de espuma blanca.
7. Quite el kit de bienvenida.
8. Quite la parte final levantando verticalmente.
9. Quite las piezas finales de madera por los cuatro botones de mano de los tornillos de la base de madera.



Caution

No deje el concentrador 2S 85" desatendido. Se necesita una persona adicional para mantener el dispositivo vertical. Una vez que se quitan las piezas finales, un mínimo de una persona debe mantener el contacto con el concentrador 2S hasta que se complete la colocación en la pared o en el carro.

10. Levantar la madera contrachapada al final de la pieza hacia arriba y hacia atrás.
11. Quite la etiqueta de relieve de atrás.
12. Levante el concentrador 2S de la bandeja inferior y colójelo en el carro o en la pared.

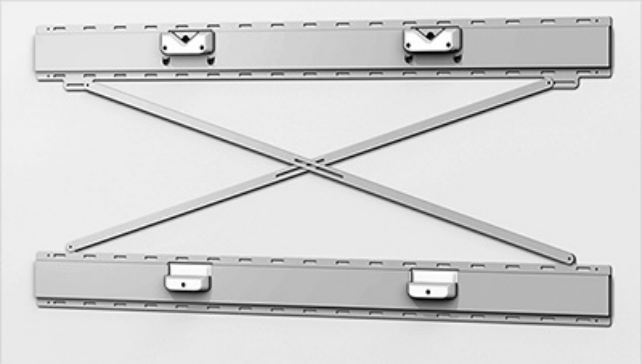
> **NOTE**
> Siguiendo las instrucciones de fabricación del carro o del montaje en pared, prepare el sistema de montaje antes de quitar el concentrador 2S de su bandeja de empaquetado interna.

> **TIP**
> Al agarrar el concentrador 2S, tenga en cuenta que la mano sujeta los recortes en la parte inferior de la espuma. Debe tener cuidado con la mano superior para no agarrar el dispositivo donde se encuentran los altavoces. El gráfico de los extremos de la cubierta del dispositivo proporciona la ubicación general del altavoz.

13. Aflojar clips de tensión elástico (x2).
14. Quite la cubierta de tela.
15. Anote las ubicaciones para colocar lápices (x2), cámara y cable de alimentación.
16. Adjunte lápices (x2), cámara y cable de alimentación.
17. Quitar etiquetas de cling (x4).
18. Presione el botón de encendido en la parte inferior derecha. La instalación ya ha finalizado.

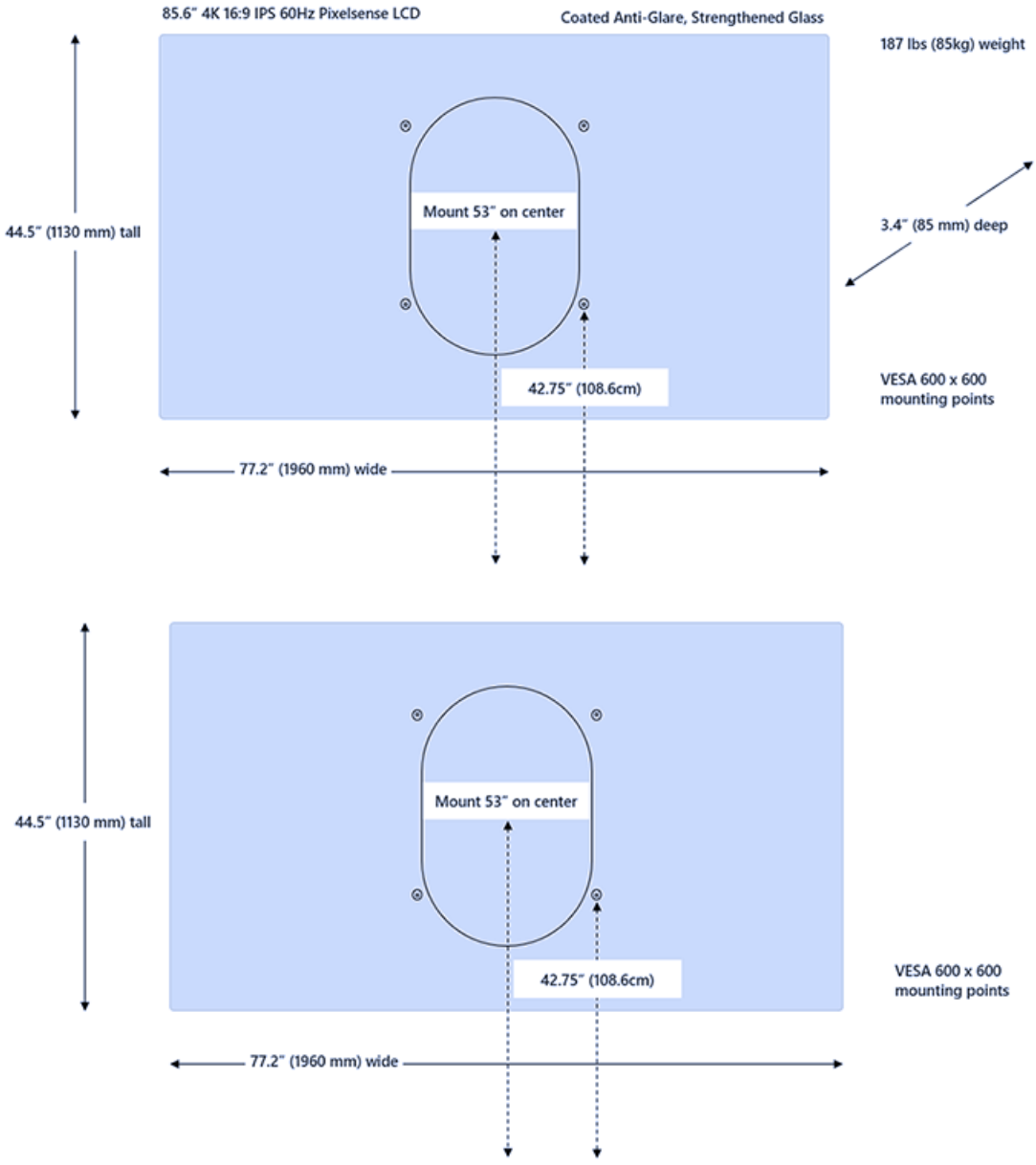
Montaje Surface Hub 2S 85"

El Surface Hub 2S 85" usa un patrón de montaje VESA de 600 x 600. Como se muestra en la siguiente imagen, Microsoft se ha asociado con Steelcase para crear opciones de montaje compatibles con el diseño único Surface Hub 2S de 85".



Dimensiones de montaje

Si usas otras opciones de montaje (que no son steelcase), necesitarás espaciadores para tener en cuenta la caja de cálculo en la parte posterior del dispositivo. Los espaciadores y otros accesorios certificados están disponibles en Salamander Designs.



Kit de fleje complementario

Se puede encontrar un conjunto adicional de materiales de fleje de empaquetado interno en el kit adjunto en la parte posterior, inferior derecha.

Apéndice A: Información de seguridad adicional

WARNING

Elevación de objetos pesados/ergonómicos

El dispositivo es muy pesado. Para reducir el riesgo de daños relacionados con el lifting, la muerte o el daño en el dispositivo, se recomienda que al menos dos o más personas levanten el dispositivo. Es importante usar una postura de elevación adecuada al levantar y/o mover el dispositivo. Use buenas prácticas de elevación ergonómicas, incluidas, entre otras, las siguientes:

- Planee con antelación. Asegúrese de que el equipo de elevación está de acuerdo con el plan.
- Determine si puede levantar la unidad. ¿Es demasiado pesado o demasiado extraño?
- Decida si necesita ayuda para levantar.
- Compruebe si hay obstáculos en el entorno y superficies resbaladizas.
- Levanta con las piernas, no con la espalda.
- Agáchate de las rodillas, manteniendo la parte posterior recta.
- Mantenga la unidad cerca del cuerpo.
- Centrar el cuerpo sobre la unidad. Mantenga separados los pies sobre el ancho del arcén.
- Levante hacia arriba sin problemas.
- Mantenga el torso recto; no se torcer al levantar o después de levantar la carga

WARNING

Montaje adecuado

El dispositivo es pesado y se conecta a un carro o montaje en la pared. Para reducir el riesgo de daño, muerte o daño al dispositivo:

- Siga todas las instrucciones proporcionadas por el fabricante del carro o montaje en pared.
- Asegúrate de que el sistema de montaje propuesto admita el peso de este dispositivo.
- Solo use el hardware de montaje proporcionado con el montaje del sistema.
- Asegúrese de que todos los tornillos se aprietan de forma segura de acuerdo con las instrucciones del fabricante.
- No libere el dispositivo hasta que esté determinado que esté totalmente comprometido con los puntos de datos adjuntos del sistema de montaje.
- Microsoft recomienda usar carros o sistemas de montaje en pared diseñados para su uso con el dispositivo. Microsoft no es responsable de ningún daño, daño o muerte causado por el uso de otros sistemas de montaje.

WARNING

Riesgos invisibles en las paredes u otras superficies de montaje

Las paredes y otras superficies de montaje pueden contener cables eléctricos, líneas de gas y otros obstáculos u obstáculos invisibles. Cortar o perforar un peligro no visto puede causar graves daños personales o la muerte. Es responsabilidad del instalador localizar los riesgos no vistos antes y evitar estos riesgos durante la instalación. Evalúe el entorno de montaje y asegúrese siempre de que no haya riesgos invisibles en la pared u otra superficie de montaje antes de la perforación o el corte.

WARNING

Peligro de sugerencia

Para evitar el riesgo de daños personales, muerte o daños en un carro o dispositivo montado en soporte cuando se mueve:

- Solo usa un carro o soporte que sea compatible con este dispositivo.
- Siga todas las instrucciones proporcionadas por el fabricante del carro/soporte para mover o reubicar un dispositivo montado en soporte.
- No cuelgue ni coloque objetos pesados desde el dispositivo ni en el carro o soporte.
- Desconecte el cable de alimentación y otros cables según sea necesario antes de mover el carro o el dispositivo montado en soporte. Tenga cuidado y muévete lentamente al mover el carro o el dispositivo montado en soporte. Siga las instrucciones del fabricante del carro/soporte para mover o reubicar el soporte.
- Tenga cuidado al transportar un carro/dispositivo montado de pie hacia arriba o hacia abajo. Nunca deje un carro o dispositivo montado de pie desatendido en o cerca de una rampa.
- Solo los adultos deben mover el carro o el dispositivo montado en soporte.

Caution

Cristal de pantalla táctil

La pantalla táctil del dispositivo, como la mayoría de las pantallas táctiles, está hecha de cristal. El cristal puede romperse si el dispositivo se deja caer o si recibe un impacto significativo. Para reducir el riesgo de daños personales, evita tocar la pantalla si el cristal está roto, astillado o roto y organiza la sustitución de la pantalla. Una pantalla táctil descomprimida o recortada causada por el uso incorrecto o el uso incorrecto del dispositivo no está cubierta por la garantía limitada del producto.

WARNING

Instalación adecuada

Para evitar riesgos relacionados con la instalación incorrecta del dispositivo, las personas que han leído y entendido la instrucción de instalación deben realizar la instalación antes de comenzar el trabajo. Si no tiene el equipamiento o la experiencia necesarios, o si no está seguro de que la superficie de montaje puede admitir correctamente consultar a un instalador profesional.

Más información

- Colección Steelcase Roam
- Diseños de salamandra

Personalizar el montaje de pared de Surface Hub 2S 50"

12/01/2022 • 3 minutes to read

En este artículo se proporcionan instrucciones para instalar físicamente el Microsoft Surface Hub 2S 50". Para obtener información acerca de la instalación de 85" vea Install and mount Surface Hub 2S 85".

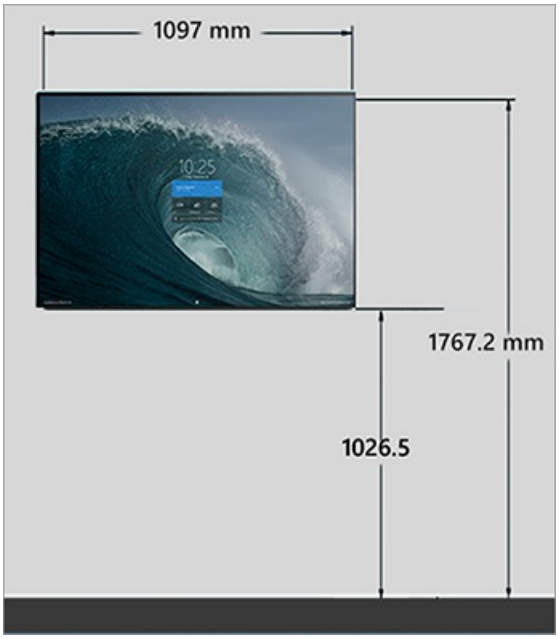
Si no usa soluciones de montaje certificadas, puede montar Surface Hub 2S 50" con hardware comercial disponible.

Establecer medidas de montaje en pared

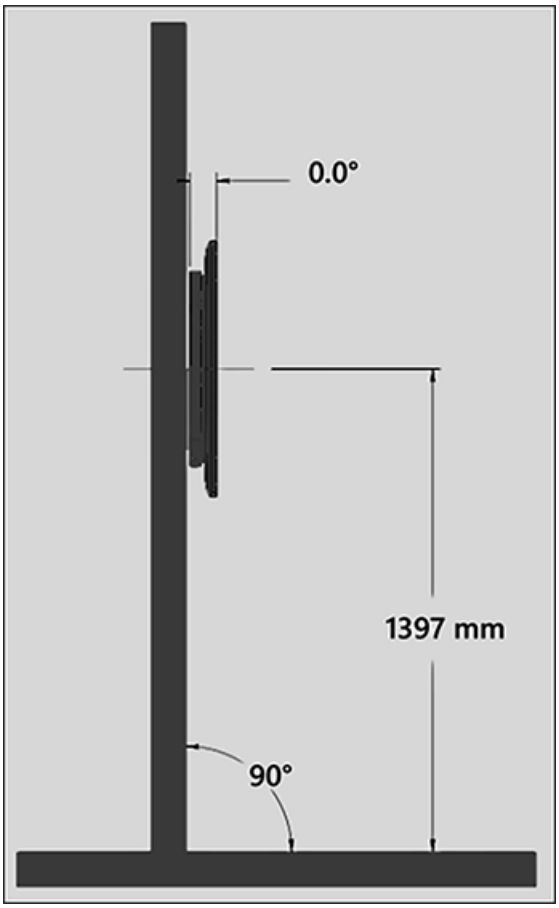
Surface Hub 2S 50" medidas de montaje recomendadas:

ELEMENTO	DESCRIPCIÓN	NOTAS
Alto desde la parte inferior Surface Hub 2S 50"	1026,5 mm (40,41")	Recomendaciones
Alto desde la parte superior Surface Hub 2S 50"	1767,2 mm (69,57")	Recomendaciones
Alto desde el centro del montaje	1397 mm (55")	Recomendaciones

1. Mida 1026,5 mm (40,41") desde el nivel del suelo para establecer la altura mínima recomendada.
2. Mida 1767,2 mm (69,57") desde el nivel del suelo para establecer la altura superior recomendada.



3. Mida 1397 mm (55") mm desde el nivel del piso para establecer la altura central recomendada.



Montaje sin obstáculos

Además de los puertos visibles en los lados del dispositivo, ciertos componentes integrados deben permanecer libres de obstáculos para funcionar correctamente. Estos incluyen los sensores Bluetooth, Wi-Fi, ocupación y micrófono, así como las ventilaciones de refrigeración térmica. Mantener fuera zonas

ELEMENTO	DESCRIPCIÓN	NOTAS
Access	Asegúrese de acceso sin intervención a los puertos de entrada y salida, el cartucho de cálculo, la radio Bluetooth, el sensor Bluetooth, la radio Wi-Fi, el sensor Wi-Fi, el sensor de ocupación.	Vea la figura 1.
Flujo de aire	Evite bloquear las zonas de ventilación de entrada y salida.	Vea la figura 2
Audio	Evite bloquear la zona de salida de audio en la parte Surface Hub 2S 50".	Vea la figura 2.

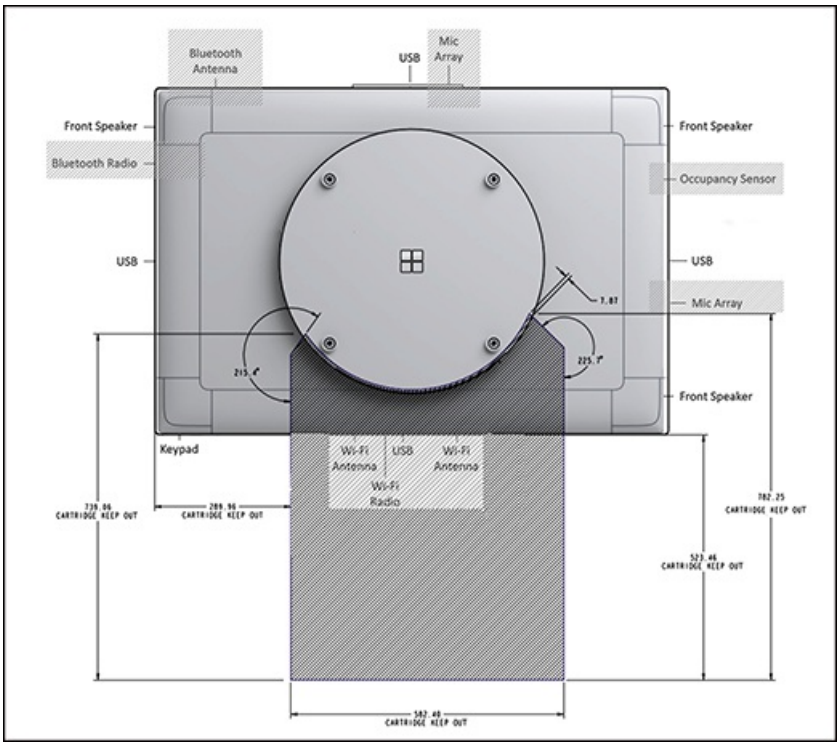


Figura 1. Mantener fuera las zonas Surface Hub componentes de 2S de 50"

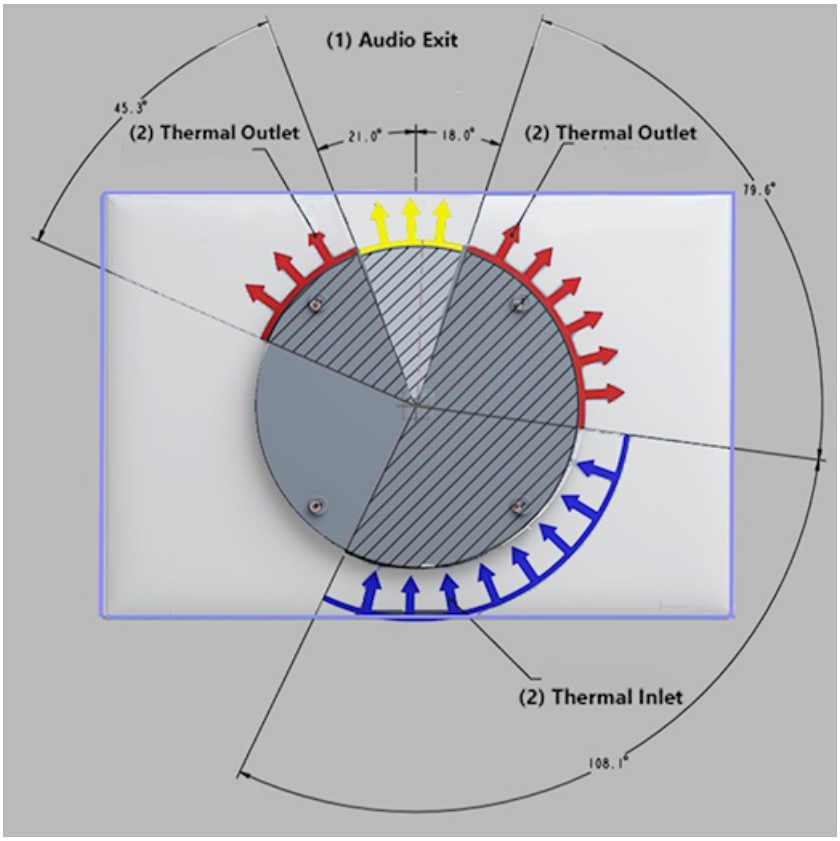


Figura 2. Evite bloquear las zonas de entrada y salida térmicas y de salida de audio.

El cartucho de cálculo extraíble que contiene los puertos de E/S debe permanecer libre de obstáculos o obstáculos de cualquier tipo.

Figura 3.View del cartucho de cálculo en la parte inferior de Surface Hub 2S 50".

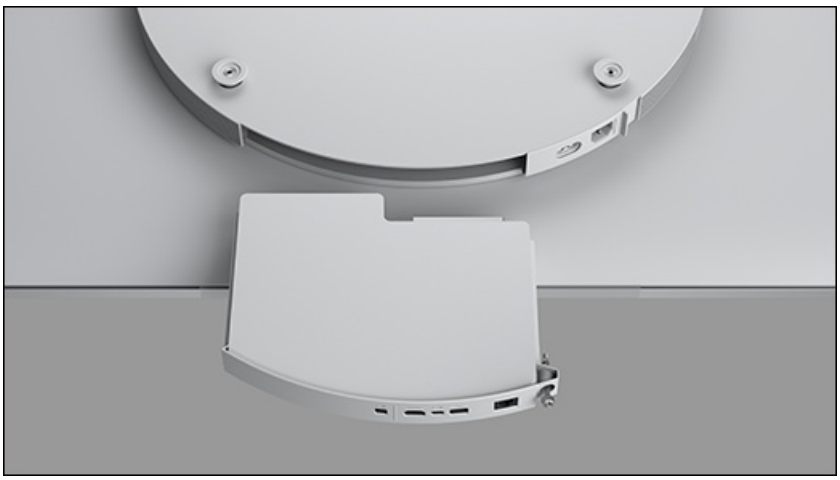


Figura 4. Eliminación sin intervención del cartucho de cálculo

Selección de un sistema de montaje

Surface Hub 2S 50" usa un marco de montaje de 350 mm x 350 mm que cumple la mayoría de los criterios enumerados en el estándar de interfaz de montaje de pantalla plana vesa. Puede instalar Surface Hub 2S 50" con cualquiera de los distintos corchetes de visualización de fuera de la plataforma diseñados para dar cabida a pantallas que difieren de las especificaciones exactas de VESA, como se muestra a continuación.

En la parte posterior de Surface Hub 2S 50", encontrarás un patrón cuadrado de cuatro agujeros con hilo M6 x 1,0 centrados en el protuberancia circular (565 mm de diámetro). Conecte el montaje con cuatro pernos métricos M6 x 1,0–12 mm de longitud. O bien, según las preferencias, puede usar pernos más largos hasta un máximo de 20 mm. Consideraciones importantes para sistemas de montaje

ELEMENTO	DESCRIPCIÓN	NOTAS
Fuerza	Solo elija montajes que puedan admitir dispositivos de al menos 28 kilos (62 lb).	Obligatorio
Rigidness	Evita montajes de pantalla flexibles que puedan disminuir la experiencia interactiva del lápiz y el uso táctil. La mayoría de los montajes de TV no están diseñados para admitir pantallas táctiles.	Recomendaciones
Profundidad	Mantenga el dispositivo bien montado en la pared, especialmente en los corredores y a lo largo de las rutas de circulación dentro de las salas.	Recomendaciones

ELEMENTO	DESCRIPCIÓN	NOTAS
Versatilidad	Asegúrese de que la solución de montaje permanece oculta de la vista tanto en el modo horizontal existente como en cualquier modo vertical potencial (sujeto a disponibilidad futura).	Recomendaciones

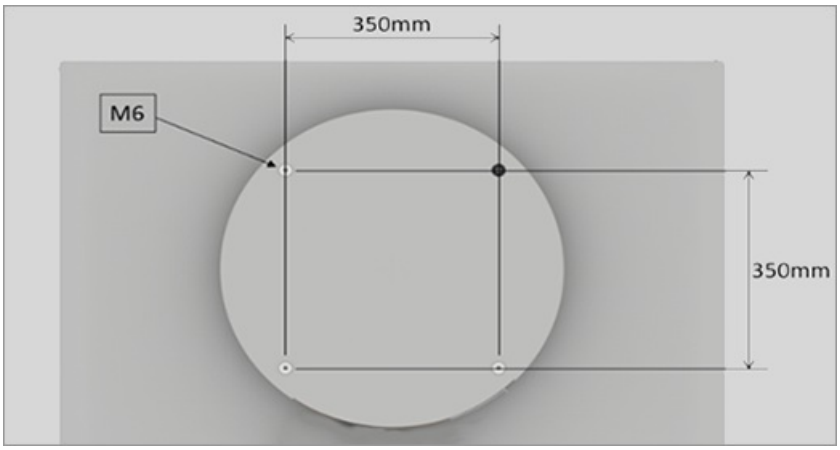


Figura 5. Surface Hub de montaje de 2S de 50"

Métodos de montaje compatibles Surface Hub 2S 50"

Surface Hub 2S 50" es compatible con montajes que permiten colocarlo en ángulos de 10-70 grados desde el plano vertical. Los montajes de riel suelen tener varios agujeros y un conjunto de ranuras, lo que permite la compatibilidad en una amplia variedad de pantallas. Un riel unido a la pared y dos montajes conectados a la pantalla permiten instalar de forma segura Surface Hub 2S 50" en una pared. Al evaluar los montajes de riel para la compatibilidad, asegúrese de que cumplen los requisitos de versatilidad enumerados anteriormente.

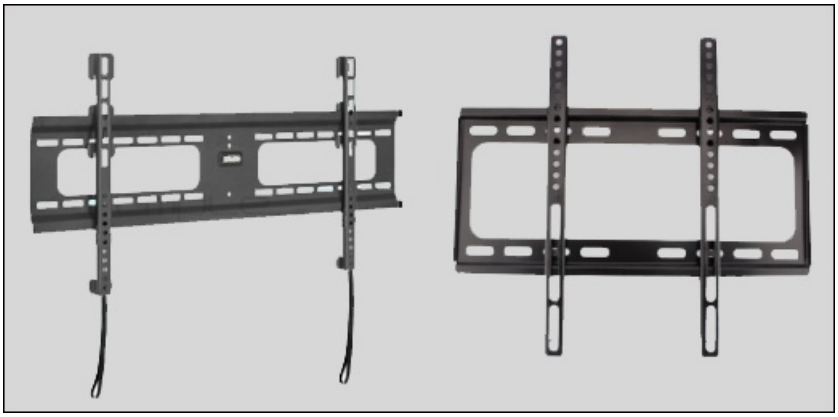


Figura 6. Surface Hub de 2S de 50"

Hoja de cálculo del programa de instalación (Surface Hub)

12/01/2022 • 8 minutes to read

Cuando hayas terminado la preinstalación y estés preparado para iniciar la primera instalación de tu Microsoft Surface Hub, asegúrate de que tienes toda la información que se muestra en esta sección.

Debes rellenar una lista para cada Surface Hub que necesitas configurar, aunque cierta información se puede usar en todos los Surface Hubs, como la información de proxy o las credenciales de dominio. Parte de esta información puede no ser necesaria, en función de cómo hayas decidido configurar el dispositivo o según cómo esté configurado el entorno de la infraestructura de la organización.

Cuando haya terminado, revise Publicar lista de comprobación de implementación a continuación.

PROPIEDAD	ESTO SE USA PARA	EJEMPLO	OBTÉN MÁS INFORMACIÓN
Información de proxy	Si usa un proxy para el acceso a Internet o de red, debe proporcionar un script o información de servidor o puerto.	Script de proxy: http://contoso/proxy.pac O: Información de servidor y puerto: 10.10.10.100, puerto 80	Configurar el proxy mediante el paquete de aprovisionamiento.
Credenciales de red inalámbrica (nombre de usuario y contraseña)	Si conecta el dispositivo a Wi-Fi y la red inalámbrica requiere credenciales de usuario.	admin1@contoso.com, #MyPassw0rd	Administración de redes inalámbricas
UPN de la cuenta del dispositivo o Dominio\nombre de usuario y la contraseña de la cuenta del dispositivo	Este es el nombre principal de usuario (UPN) o el dominio\nombre de usuario y la contraseña de la cuenta del dispositivo. El correo, el calendario, Microsoft Teams y Skype Empresarial dependen de una cuenta de dispositivo compatible.	UPN: ConfRoom15@contoso.com, #Passw0rd1 O: Dominio y nombre de usuario: CONTOSO\ConfRoom15, #Passw0rd1	Crear y probar una cuenta de dispositivo
Propiedades del buzón	El buzón de correo debe estar configurado con las propiedades correctas para obtener la mejor experiencia de reunión en Surface Hub.	Vea Propiedades Exchange Microsoft	

PROPIEDAD	ESTO SE USA PARA	EJEMPLO	OBTÉN MÁS INFORMACIÓN
DIRECCIÓN URL de EWS para el buzón de la cuenta de dispositivo	Este es el servidor Exchange de la cuenta del dispositivo. El correo, el calendario, Microsoft Teams y Skype Empresarial dependen de una cuenta de dispositivo compatible. Para que el correo electrónico y el calendario funcionen, la cuenta del dispositivo debe tener un servidor Exchange válido. El dispositivo intentará encontrar esto automáticamente.	https://outlook.office365.com/EWS/exchange.asmx	Crear y probar una cuenta de dispositivo Propiedades de Microsoft Exchange
Dirección de Protocolo de inicio de sesión (SIP) de la cuenta del dispositivo	Esta es la dirección SIP de la cuenta del dispositivo. El correo, el calendario, Microsoft Teams y Skype Empresarial dependen de una cuenta de dispositivo compatible. Para que los equipos o Skype empresa funcionen, la cuenta del dispositivo debe tener una dirección SIP válida El dispositivo intentará encontrarlo automáticamente.	sip: ConfRoom15@contoso.com	
Contraseña de la cuenta de dispositivo	Para simplificar la administración, puedes deshabilitar la expiración de contraseña para la cuenta del dispositivo o permitir Surface Hub girar automáticamente la contraseña de la cuenta del dispositivo. **Nota:** Si agrega la cuenta en formato dominio\nombredeusuario, afilia el Concentrador a Active Directory local durante la instalación inicial. Si agrega la cuenta en username@domain.com, afilia el concentrador con Azure Active Directory durante la configuración inicial. De lo contrario, la rotación de contraseñas no funcionará.		Administración de contraseñas
Exchange Servicios web (EWS)	Habilitar EWS. Surface Hub usa EWS para sincronizar su calendario.		Autenticación moderna en Surface Hub

PROPIEDAD	ESTO SE USA PARA	EJEMPLO	OBTÉN MÁS INFORMACIÓN
Autenticación multifactor	Deshabilita la autenticación multifactor en la cuenta del dispositivo. Como el Surface Hub inicia sesión Exchange en segundo plano sin la interacción del usuario, no puede responder a ningún mensaje interactivo, como la autenticación multifactor.		
Detalles de inscripción de MDM	Si quieres inscribir manualmente el dispositivo en MDM, deberás tener credenciales de usuario válidas para el proveedor mdm y la dirección URL de inscripción. El dispositivo intentará encontrar la dirección URL de inscripción automáticamente.	manage.microsoft.com	Administrar Surface Hub con un proveedor MDM
Nombre descriptivo	El nombre descriptivo del dispositivo es el nombre de emisión que los usuarios verán cuando intenten conectarse de forma inalámbrica al Surface Hub. Este nombre se mostrará de forma destacada en la pantalla del Surface Hub. Se recomienda que el nombre descriptivo que elijas sea reconocible y único para que los usuarios puedan distinguir un Surface Hub de otro al intentar conectarse.	Sala de conferencias 15	Configuración por primera vez para Surface Hub
Nombre de dispositivo	El nombre del dispositivo es el nombre que se usará para unirse a un dominio y es la identidad que verás en el proveedor MDM si el dispositivo está inscrito en el MDM. El nombre del dispositivo que elijas no debe ser el mismo nombre que cualquier otro dispositivo del dominio de Active Directory (si decides unirte al dispositivo en el dominio). El dispositivo no puede unirse al dominio sin un nombre único.	confroom15	Configuración por primera vez para Surface Hub

PROPIEDAD	ESTO SE USA PARA	EJEMPLO	OBTÉN MÁS INFORMACIÓN
Modo de aplicación de Teams	- Modo 0: Skype Empresarial con Microsoft Teams funcionalidad para reuniones programadas. - Modo 1: Microsoft Teams con Skype Empresarial funcionalidad para reuniones programadas. - Modo 2: Microsoft Teams solo		Cambiar la plataforma de comunicaciones empresariales predeterminada

Afiliación de dispositivos

Usa la afiliación a dispositivos para administrar el acceso de los usuarios a Configuración aplicación en Surface Hub. Con el Windows 10 Team operativo (que se ejecuta en Surface Hub), solo los usuarios autorizados pueden ajustar la configuración con la Configuración aplicación. Dado que elegir la afiliación puede afectar a la disponibilidad de las características, planee correctamente para garantizar que los usuarios puedan acceder a las características según lo previsto.

> **NOTE**
> Solo puedes establecer la afiliación de dispositivos durante la configuración inicial de la experiencia de inicio de la caja (OOBE). Si necesitas restablecer la afiliación a dispositivos, tendrás que repetir la configuración de OOBE.

Si te unes a Azure AD

PROPIEDAD	ESTO SE USA PARA	EJEMPLO	OBTÉN MÁS INFORMACIÓN
Credenciales de usuario de inquilino de Azure AD (nombre de usuario y contraseña)	Si decide que los usuarios de la organización de Azure Active Directory (Azure AD) se conviertan en administradores en el dispositivo, deberá unirse a la Surface Hub a Azure AD. Para unirse a Azure AD, necesitará credenciales válidas para una cuenta en el inquilino.	admin1@contoso.com, #MyPassw0rd	Administración del grupo de administradores
Cuentas de administrador no globales	Para Surface Hub unidos a Azure AD, puede limitar los permisos de administración a la administración de la aplicación Configuración en Surface Hub. Esto le permite tener en cuenta los permisos de administración Surface Hub y evitar el acceso de administrador potencialmente no deseado a todo un dominio de Azure AD.		Configurar cuentas de administrador no globales en Surface Hub

Si se une a un dominio

PROPIEDAD	ESTO SE USA PARA	EJEMPLO
Dominio al que unirse	Este es el dominio al que debes unirte para que un grupo de seguridad de tu elección pueda ser administrador del dispositivo. Es posible que necesites el nombre de dominio completo (FQDN).	contoso (nombre corto) O contoso.corp.com (FQDN)
Credenciales de cuenta de dominio (nombre de usuario y contraseña)	No puedes unirte a un dominio a menos que proporciones las credenciales de cuenta suficientes para unirte al dominio. Una vez que proporciones un dominio al que unirte y las credenciales para unirte al dominio, un grupo de seguridad de tu elección podrá cambiar la configuración del dispositivo.	admin1, #MyPassw0rd
Alias del grupo de seguridad de administrador	Este es un grupo de seguridad de tu Active Directory (AD); todos los miembros de este grupo de seguridad pueden cambiar la configuración del dispositivo.	SurfaceHubAdmins

Si usa un administrador local

PROPIEDAD	ESTO SE USA PARA	EJEMPLO
Credenciales de cuenta de administrador local (nombre de usuario y contraseña)	Si no quieres unirte a un dominio de AD o a Azure AD, puedes crear una cuenta de administrador local en el dispositivo.	admin1, #MyPassw0rd

Si necesitas instalar certificados o aplicaciones

PROPIEDAD	ESTO SE USA PARA
Unidad USB	Si sabes antes de ejecutar por primera vez que quieres instalar certificados o aplicaciones universales, sigue los pasos de Crear paquetes de aprovisionamiento para Surface Hub. Los paquetes de aprovisionamiento se crearán en una unidad USB.

Lista de comprobación posterior a la implementación

COMPROBADO	RESPUESTA
Sincronización de cuentas de dispositivo	☐ Sí ☐ No
Clave de Bitlocker	☐ guardado en archivo (sin afiliación) ☐ guardado en Active Directory (afiliación a AD) ☐ guardado en Azure AD (afiliación a Azure AD)

COMPROBADO	RESPUESTA
Actualizaciones del sistema operativo del dispositivo	☐ completado
Windows Actualizaciones de la Tienda	☐ automático ☐ manual
Microsoft Teams reunión programada	☐ correo electrónico de confirmación recibido ☐ reunión aparece en la pantalla de inicio ☐ de unión con un solo toque ☐ puede unirse al audio ☐ puede unirse al vídeo ☐ puede compartir pantalla
Skype Empresarial reunión programada	☐ correo electrónico de confirmación recibido ☐ reunión aparece en la pantalla de inicio ☐ funciones de unión con un solo toque correctamente ☐ puede unirse al audio ☐ puede unirse al vídeo ☐ puede compartir pantalla ☐ puede enviar/recibir mensajería instantánea
Reunión programada cuando ya está invitada	☐ de reunión rechazada
Microsoft Teams reunión ad-hoc	☐ invitar a otros usuarios a trabajar ☐ puede unirse al audio ☐ puede unirse al vídeo ☐ puede compartir pantalla
Microsoft Whiteboard	☐ inicio desde la pantalla Inicio /Inicio ☐ iniciar desde Microsoft Teams
Llamada Teams/Skype entrante	☐ puede unirse al audio ☐ puede unirse al vídeo ☐ puede compartir pantalla ☐ puede enviar/recibir mi mi (solo Skype Empresarial)
Secuencias de vídeo en directo entrantes	☐ máximo 2 (Skype Empresarial) ☐ máximo 4 (Microsoft Teams)
Microsoft Teams Comportamiento del modo 0	☐ Skype Empresarial icono en la pantalla Inicio/Inicio ☐ puede unirse a reuniones Skype Empresarial programadas (Skype interfaz de usuario) ☐ puede unirse a reuniones Teams programadas (Teams interfaz de usuario)

COMPROBADO	RESPUESTA
Microsoft Teams Comportamiento del modo 1	☐ Teams en la pantalla Inicio/Inicio ☐ puede unirse a reuniones Skype Empresarial programadas (Skype interfaz de usuario) ☐ puede unirse a reuniones Teams programadas (Teams interfaz de usuario)
Microsoft Teams Comportamiento del modo 2	☐ Teams icono en la pantalla Inicio /Inicio ☐ puede unirse a reuniones Teams programadas ☐ no poder unirse a Skype Empresarial reuniones

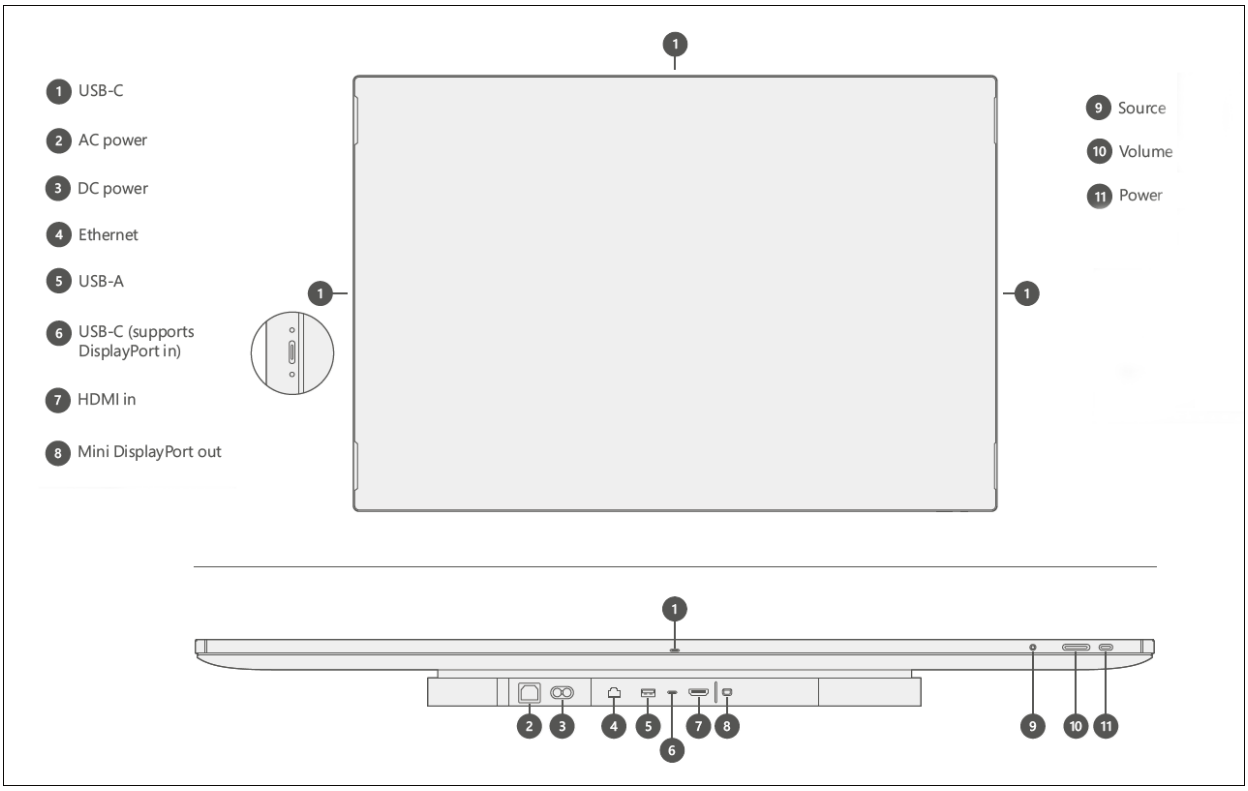
Introducción a los puertos y el teclado numérico de Surface Hub 2S

12/01/2022 • 2 minutes to read

En esta página se describen los puertos, los botones físicos y la información de configuración esenciales para conectarse a Surface Hub 2S, ya sea a través de métodos con cable, Wi-Fi o Bluetooth configuración. También incluye recomendaciones de procedimientos recomendados para escenarios clave de conectividad.

> **NOTE**
>
> Puedes encontrar el número de serie en el exterior del empaquetado, en la pantalla por el cable de alimentación o mediante la aplicación Surface.

En la figura siguiente se muestra la ubicación de los puertos y los botones físicos en un teclado conectado a la parte inferior del dispositivo. La tabla incluye descripciones detalladas de cada elemento.

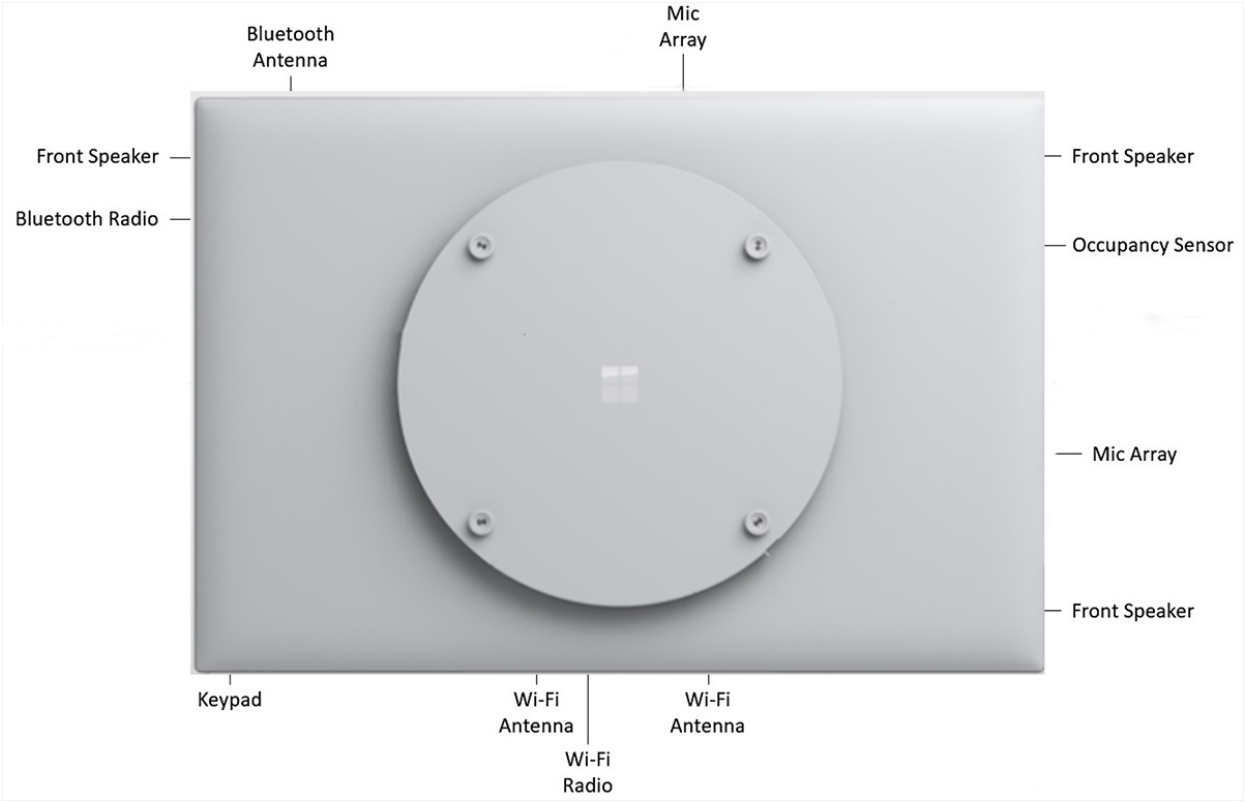


Referencia de componentes de teclado y puerto

KEY	COMPONENTE	DESCRIPCIÓN	PARÁMETROS CLAVE

KEY	COMPONENTE	DESCRIPCIÓN	PARÁMETROS CLAVE
1	**USB C**	**USB 3.1 Gen 1** Úselo como puerto de acceso para conectar periféricos, como unidades usb. Los puertos invitados están en cada lado del dispositivo (4). *NOTA: Este es el puerto recomendado para conectar una cámara externa. Las características de montaje de cámara adicionales se incorporan al diseño para ayudar a admitir la retención de cámaras conectadas.* NOTA: TouchBack y la ingesta de vídeo no se admiten en estos puertos.	Tipo C Puerto de 15 W (5V/3A)
2	**Alimentación de CA**	**Entrada de 100 a 240 V** Conectar a la alimentación de CA estándar y Surface Hub 2S cambiarán automáticamente al estándar de energía local, como 110 volts en Estados Unidos y Canadá o 220 volts en el Reino Unido.	IEC 60320 C14
3	**Alimentación de CC**	**Puerto de entrada dc de 24V** Se usa para conectarse a la batería móvil.	Xbox1 Dual barrel to Anderson connector
4	**Ethernet**	**1000/100/10 Base-T** Se usa para proporcionar una conexión continua en un entorno corporativo y escenarios relacionados que requieren la máxima estabilidad o capacidad.	RJ45
5	**USB-A**	**USB 3.1 Gen 1** Úselo como puerto de acceso para conectar periféricos, como unidades usb.	Tipo A Puerto de 7,5 W (5V/1,5A)

KEY	COMPONENTE	DESCRIPCIÓN	PARÁMETROS CLAVE
6	**USB-C**	**USB 3.1 Gen 1** Úselo como puerto de acceso para conectar equipos externos y dispositivos relacionados o conectar periféricos, como unidades digitales. *NOTA: Este es el puerto de entrada recomendado para vídeo, TouchBack y InkBack.*	Tipo C Puerto de 18 W (5V/3A, 9V/2A)
7	**HDMI-in**	**HDMI 2.0, HDCP 2.2 /1.4** Se usa para varios escenarios, incluida la entrada de invitado HDMI a HDMI.	HDMI estándar
8	**Mini DP-out**	**Salida Mini DP 1.2** Se usa para escenarios de salida de vídeo, como la creación Surface Hub pantalla 2S en un proyector más grande. *NOTA: Esto admite una resolución máxima de 3840 x 2160 (4K UHD) @60Hz.*	Mini DP
9	**Source**	Se usa para alternar entre orígenes de ingesta conectados: modos de PC externo, HDMI y Mini DP.	n/d
10	**Volumen**	Usa +/- para ajustar el audio localmente en el dispositivo. *NOTA: Cuando vaya al control de brillo, use +/- en el control deslizante de volumen para controlar el brillo de la pantalla.*	n/d
11	**Inicio/apagado**	Encienda y apague el dispositivo. Úselo también para navegar por los menús para mostrar y seleccionar elementos.	n/d


Bluetooth Antenna
Mic Array
Front Speaker
Bluetooth Radio
Front Speaker
Occupancy Sensor
Mic Array
Front Speaker
Keypad
Wi-Fi Antenna
Wi-Fi Radio
Wi-Fi Antenna

Preparar el entorno para Microsoft Surface Hub

12/01/2022 • 5 minutes to read

En esta página se describen las dependencias para configurar y administrar Surface Hub v1 o Surface Hub 2S.

Dependencias de infraestructura

Revisa estas dependencias para asegurarte de que las características de Surface Hub funcionarán en tu infraestructura de TI.

DEPENDENCIA	DESCRIPCIÓN	OBTÉN MÁS INFORMACIÓN
Servicios locales y Active Directory o M365	Surface Hub usa una cuenta de Active Directory o Azure AD (denominada cuenta de **dispositivo)** para obtener acceso a Exchange y Teams (o Skype Empresarial). Surface Hub debe ser capaz de conectarse al controlador de dominio de Active Directory o al inquilino de Azure AD para validar las credenciales de la cuenta del dispositivo, así como para acceder a información como el nombre para mostrar de la cuenta del dispositivo, el alias, el servidor Exchange y la dirección de Protocolo de inicio de sesión (SIP). **NOTA: Surface Hubs funciona con Microsoft Teams, Skype Empresarial Server 2019, Skype Empresarial Server 2015 o Skype Empresarial Online. No se admiten plataformas anteriores, como Lync Server 2013. Los Surface Hubs no se admiten GCC entornos De alto o DoD.**	Microsoft 365 de conexión Crear y probar una cuenta de dispositivo
Windows Actualización, almacenamiento y diagnóstico	El acceso a Windows Update o Windows Update para empresas es necesario para mantener Surface Hub actualizaciones de calidad y características del sistema operativo. El acceso a la Microsoft Store es necesario para mantener las aplicaciones.	Administrar puntos de conexión de conexión para Windows 10 Enterprise, versión 20H2 Administrar actualizaciones de Windows en Surface Hub
Solución de administración de dispositivos móviles (MDM) (Microsoft Intune, Microsoft Endpoint Configuration Manager o proveedor MDM compatible con terceros)	Si quieres aplicar la configuración e instalar las aplicaciones de forma remota, y hacerlo en varios dispositivos a la vez, debes configurar una solución MDM e inscribir el dispositivo en dicha solución.	Puntos de conexión de la red para Microsoft Intune Administrar la configuración con un proveedor de MDM

DEPENDENCIA	DESCRIPCIÓN	OBTÉN MÁS INFORMACIÓN
Azure Monitor	Azure Monitor se puede usar para supervisar el estado de Surface Hub dispositivos. **NOTA: Los Surface Hubs no admiten actualmente el uso de un servidor proxy para comunicarse con el servicio log analytics que usa Azure Monitor.**	Puntos de conexión de Log Analytics Supervisar Surface Hubs con Azure Monitor para realizar un seguimiento de su estado.
Acceso a la red	Los Surface Hub admiten conexiones cableadas o inalámbricas (se prefiere una conexión por cable). **Autenticación 802.1X** En Windows 10 Team 20H2, aunque la autenticación 802.1X para conexiones cableadas e inalámbricas está habilitada de forma predeterminada, debe asegurarse de que un certificado de autenticación y perfil de red 802.1x también esté instalado en Surface Hub. Si administras Surface Hub intune u otra solución de administración de dispositivos móviles, puedes entregar el certificado mediante el CSP ClientCertificateInstall. De lo contrario, puedes crear un paquete de aprovisionamiento e instalarlo durante la instalación de la primera ejecución o mediante la Configuración aplicación. Cuando se aplica el certificado, la autenticación 802.1X comienza automáticamente. **IP dinámica** Surface Hubs no se puede configurar para usar una IP estática. Se les debe asignar una dirección IP a través de DHCP. **Puertos** El Surface Hub requiere los siguientes puertos abiertos: HTTPS: 443 HTTP: 80 NTP: 123	Habilitar la autenticación por cable 802.1x Crear paquetes de aprovisionamiento para Surface Hub

Afiliación de dispositivos

Usa la afiliación a dispositivos para administrar el acceso de los usuarios a Configuración aplicación en Surface Hub. Con el Windows 10 Team operativo (que se ejecuta en Surface Hub), solo los usuarios autorizados pueden ajustar la configuración con la Configuración aplicación. Dado que elegir la afiliación puede afectar a la disponibilidad de las características, planee correctamente para garantizar que los usuarios puedan acceder a las características según lo previsto.

> **NOTE**
> Solo puedes establecer la afiliación de dispositivos durante la configuración inicial de la experiencia de inicio de la caja (OOBE). Si necesitas restablecer la afiliación a dispositivos, tendrás que repetir la configuración de OOBE.

Sin afiliación

Ninguna afiliación es como tener Surface Hub en un grupo de trabajo con una cuenta de administrador local diferente en cada Surface Hub. Si eliges Sin afiliación, debes guardar localmente la clave de BitLocker en una unidad usb. Todavía puedes inscribir el dispositivo con Intune; sin embargo, solo el administrador local puede acceder a la Configuración con las credenciales de cuenta configuradas durante OOBE. Puedes cambiar la contraseña de la cuenta de administrador desde la Configuración aplicación.

Active Directory Domain Services

Si te afilias Surface Hub con los Servicios de dominio de Active Directory locales, debes administrar el acceso a la aplicación Configuración mediante un grupo de seguridad en tu dominio. Esto ayuda a garantizar que todos los miembros del grupo de seguridad tengan permisos para cambiar la configuración en Surface Hub. Tenga en cuenta lo siguiente: cuando Surface Hub filiales con los Servicios de dominio de Active Directory locales, la clave de BitLocker se puede guardar en el esquema de Active Directory. Para obtener más información, vea Prepare your organization for BitLocker: Planning and policies.

Las CA raíz de confianza de la organización se insertan en el mismo contenedor de Surface Hub, lo que significa que no es necesario importarlas mediante un paquete de aprovisionamiento.

Todavía puedes inscribir el dispositivo con Intune para administrar la configuración de forma centralizada en tu Surface Hub.

Azure Active Directory

Cuando eliges asociar tu Surface Hub con Azure Active Directory (Azure AD), cualquier usuario con el rol Administrador global puede iniciar sesión en la aplicación Configuración en Surface Hub. También puedes configurar cuentas de administrador no globales que limiten los permisos a la administración de la aplicación Configuración en Surface Hub. Esto te permite tener en cuenta los permisos de administrador solo para Surface Hubs y evitar el acceso de administrador potencialmente no deseado en todo un dominio de Azure AD.

Si habilitaste la inscripción automática de Intune para tu organización, el Surface Hub se inscribirá automáticamente en Intune; en este escenario, la cuenta usada para la afiliación de Azure AD durante la instalación debe tener licencia para Intune y tener permisos para inscribir Windows dispositivos. Una vez completado el proceso de configuración, la clave BitLocker del dispositivo se guarda automáticamente en Azure AD.

Para obtener más información sobre cómo administrar Surface Hub con Azure AD, consulte:

- Administración del grupo de administradores
- Configurar cuentas de administrador no globales en Surface Hub

Revisar y completar la hoja de cálculo del programa de instalación de Surface Hub (opcional)

Cuando sigas los pasos del programa de primera ejecución de Surface Hub, tendrás que proporcionar determinada información. La hoja de cálculo del programa de instalación resume esa información y proporciona listas de información específica del entorno que necesitarás cuando sigas los pasos del programa de primera ejecución. Para obtener más información, consulta Hoja de cálculo del programa de instalación.

Guías de adopción y formación de Surface Hub 2

12/01/2022 • 2 minutes to read

Ya sea que sea una empresa pequeña o grande, un plan de adopción de Surface Hub es fundamental para generar los casos de uso correctos y ayudar a los usuarios a sentirse cómodos con el dispositivo. Consulte estas guías descargables diseñadas para ayudarle a ofrecer formación en toda la organización.

Formación a petición

- Vídeos de adopción y formación de Surface Hub 2S

Kit de herramientas de adopción

- Kit de herramientas de adopción de Surface Hub

Guías de aprendizaje

- Guía de aprendizaje: usuario final
- Guía de aprendizaje: usuario avanzado
- Guía de aprendizaje: servicio de asistencia
- Guía de aprendizaje: escritorio de Microsoft Teams

Descargar todas las guías de aprendizaje

Guías para el usuario final

- Guía para la navegación en Surface Hub
- Guía de Office 365 en Surface Hub
- Guía de Microsoft whiteboard en Surface Hub
- Guía de Microsoft Teams en Surface Hub

Descargar todas las guías para el usuario final

Tarjetas de referencia rápida

- Conectar el equipo
- Unirse a una reunión de Teams
- Administrar una reunión de Teams
- Conceptos básicos de navegación
- Programar una reunión de Teams
- Iniciar una reunión nueva de Teams
- Compartir o enviar un archivo
- Iniciar sesión para ver las reuniones y los archivos
- Pizarra avanzada
- Herramientas de pizarra

Descargar todas las tarjetas de referencia rápida

Vídeos de formación y adopción a petición de Surface Hub 2S

12/01/2022 • 2 minutes to read

Esta página contiene una formación completa sobre Surface Hub 2S, disponible a petición.

Capítulo 1: información general de aprendizaje

- Bienvenida e introducción
- Información general de aprendizaje y agenda
- Referencia de software y tecnología
- Mensajería de Surface Hub
- Sectores y roles de usuario
- Información general de los servicios de formación
- Procedimientos recomendados para la formación

Capítulo 2: Introducción a Surface Hub

- ¿Qué es Surface Hub?
- Información general técnica
- Steelcase roaming y la historia de la movilidad
- Servicios Surface Hub
- Introducción a Surface Hub
- Recopilar las expectativas

Capítulo 3: navegación de Surface Hub

- Pantalla de inicio de sesión
- Menú Inicio
- Pantalla completa
- Imagen prediseñada a pizarra
- Menú de la barra de tareas
- Teams/Skype
- Finalizar sesión

Capítulo 4: pizarras y colaboración

- Introducción a la pizarra
- Iniciar la pizarra
- Herramientas de pizarra
- Insertar imágenes

- Cambiar el fondo
- Compartir la pizarra
- Exportar la pizarra

Capítulo 5: explorar las aplicaciones de Surface Hub

- Introducción a las aplicaciones Surface Hub
- Introducción a PowerPoint
- Microsoft Word
- Microsoft Excel
- Microsoft Edge

Capítulo 6: aplicaciones avanzadas y Office 365

- Introducción a las aplicaciones avanzadas
- Mapas de Microsoft
- Fotos
- Power BI
- Inicia sesión en Office 365
- OneDrive
- Documentos con coautoría

Capítulo 7: conectar dispositivos

- Introducción a Connect
- Información general de Miracast
- Entrada táctil y de lápiz
- Descripción general de conexión cableada
- Flujos de trabajo de la aplicación de línea de negocio
- Solución de problemas de Miracast y conexión por cable

Capítulo 8: reuniones de Skype empresarial

- Introducción a Skype empresarial: programación de reuniones de Skype empresarial
- Iniciar una reunión
- Iniciar una reunión ad hoc
- Unirse a una reunión en el calendario
- Administrar una reunión de Skype empresarial
- Presentar contenido

Capítulo 9: reuniones de Microsoft Teams

- Introducción a Microsoft Teams
- Programación de reuniones de Microsoft Teams

- Iniciar una reunión
- Iniciar una reunión ad hoc
- Unirse a una reunión en el calendario
- Administrar una reunión de Microsoft Teams
- Presentar contenido
- Conclusión

Capítulo 10: solución de problemas básicos

- Introducción a la solución de problemas de Surface Hub
- Solución de problemas de aplicaciones
- Finalizar sesión
- Reiniciar el dispositivo
- Encender y apagar el dispositivo
- Restablecimiento de fábrica
- Configuración
- Administrar Surface Hub
- Conclusión

Configuración por primera vez para Surface Hub

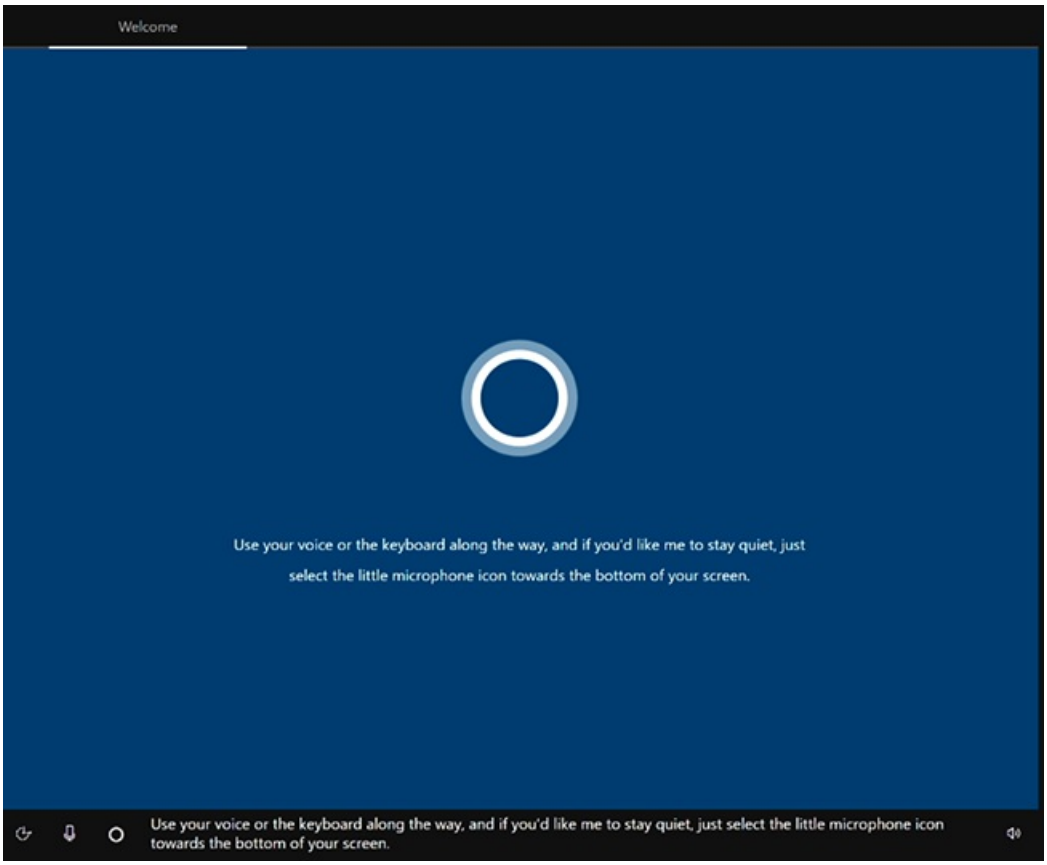
12/01/2022 • 4 minutes to read

La primera vez que Surface Hub, el dispositivo entra automáticamente en el modo de configuración por primera vez para guiarte a través de la configuración de la cuenta y la configuración relacionada.

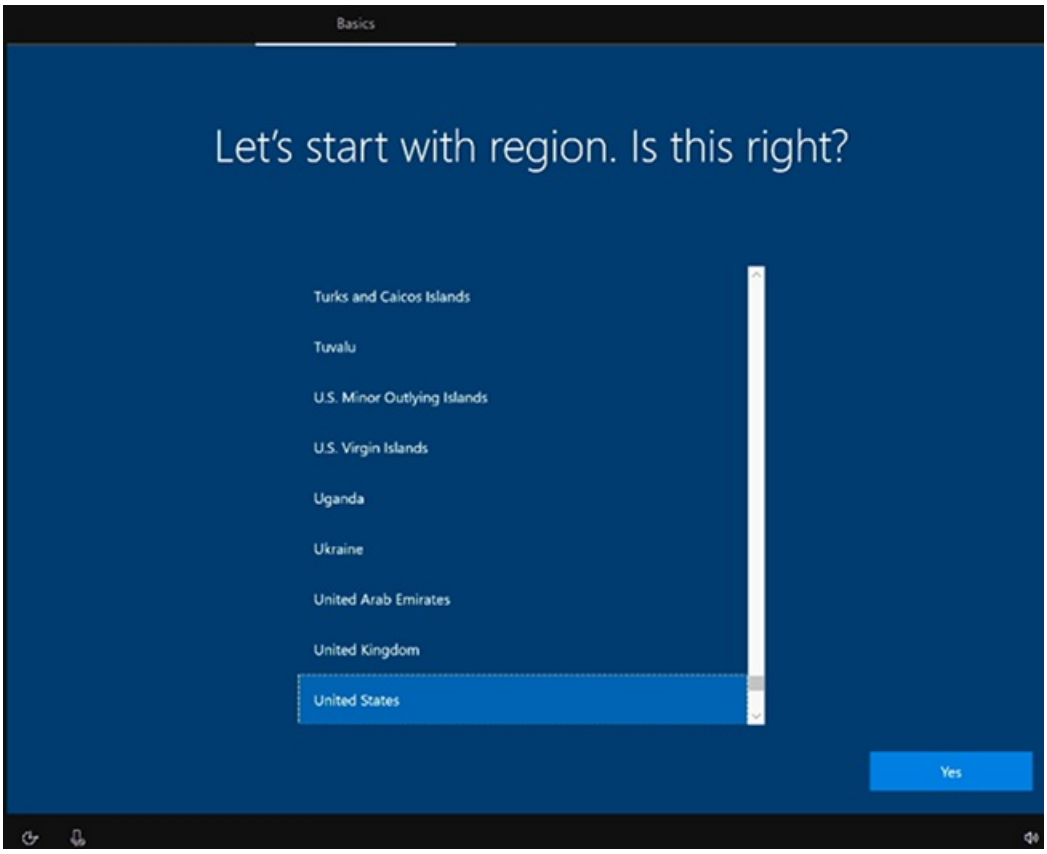
> **TIP**
> Puedes automatizar todo el proceso de configuración con un paquete de aprovisionamiento para garantizar una experiencia coherente en varios Surface Hubs.

Comenzar

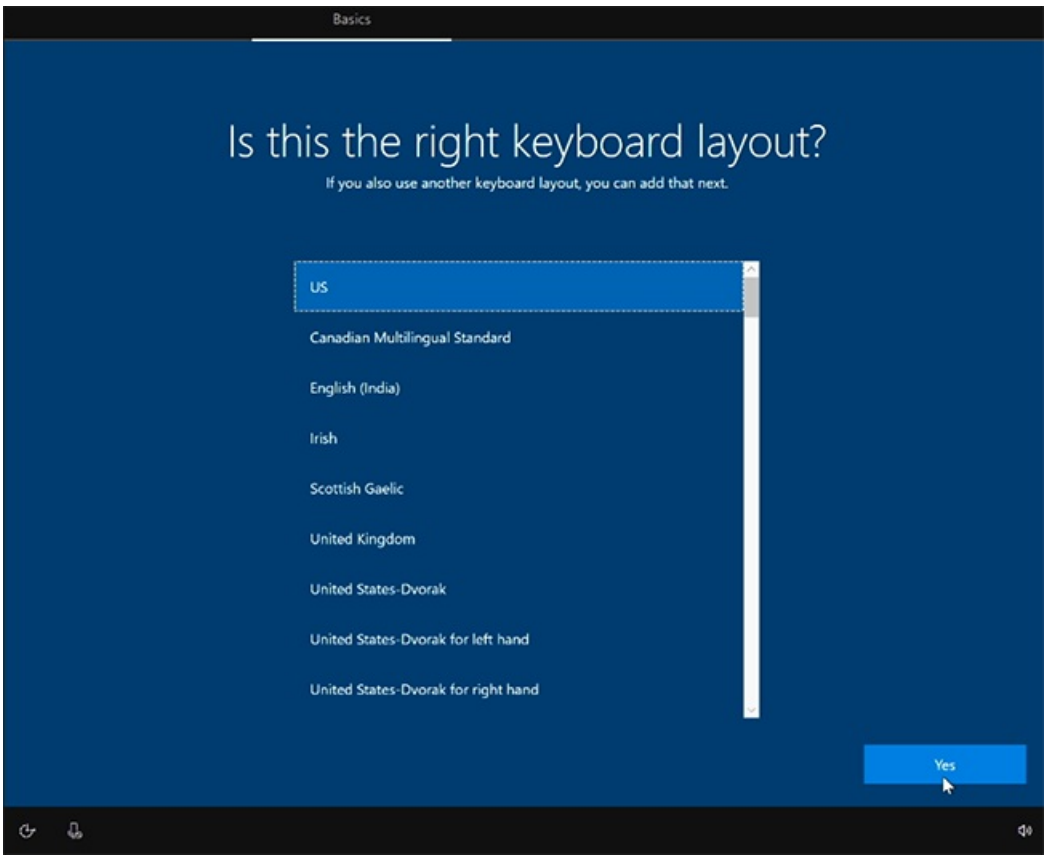
1. De forma predeterminada, Cortana está habilitado para guiarlo a través del proceso. Para desactivar la Cortana, seleccione el icono del micrófono.



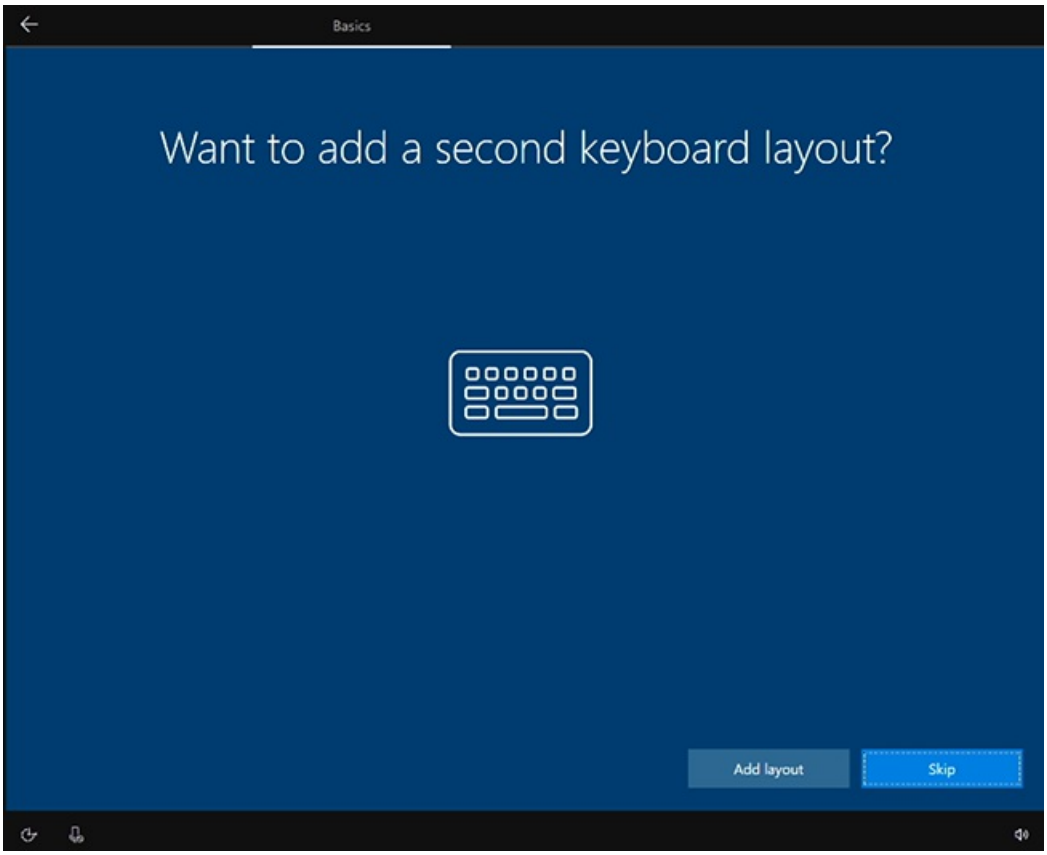
2. **Elige tu región.** Confirme la región detectada automáticamente y seleccione **Sí**.



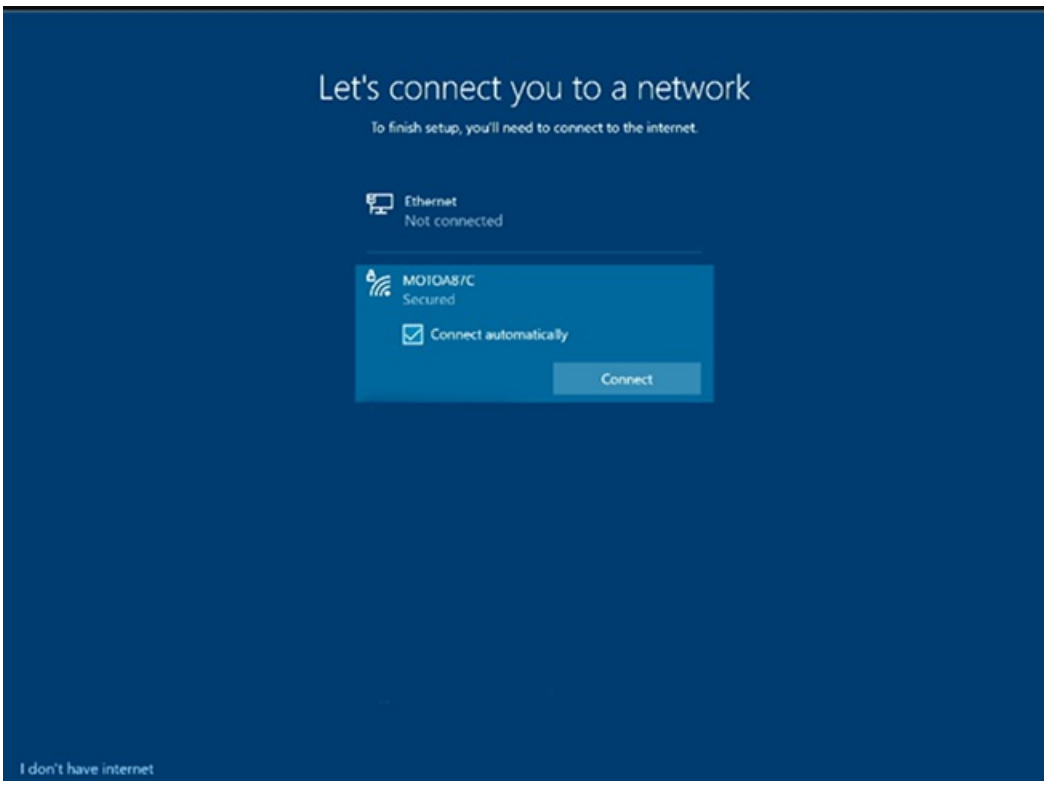
3. **Confirme el diseño del teclado.** Seleccione **Sí**.



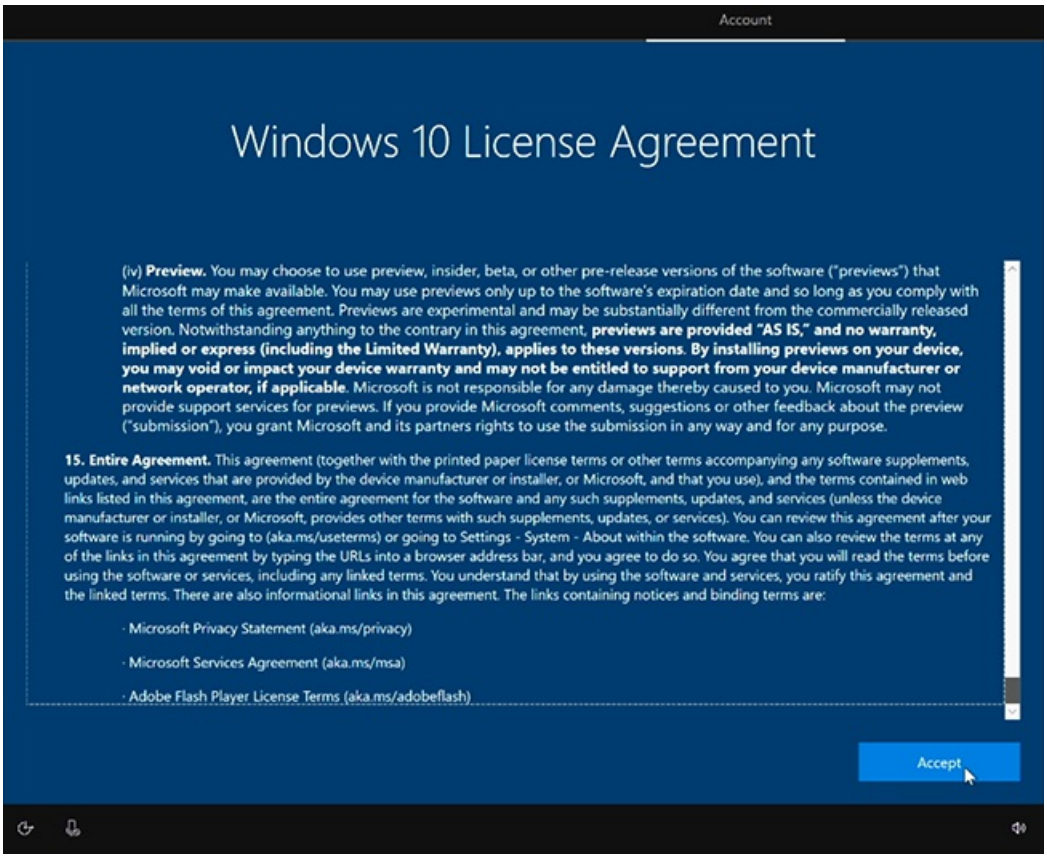
4. Para agregar un segundo teclado, seleccione **Agregar diseño**. De lo contrario, **seleccione Omitir**.



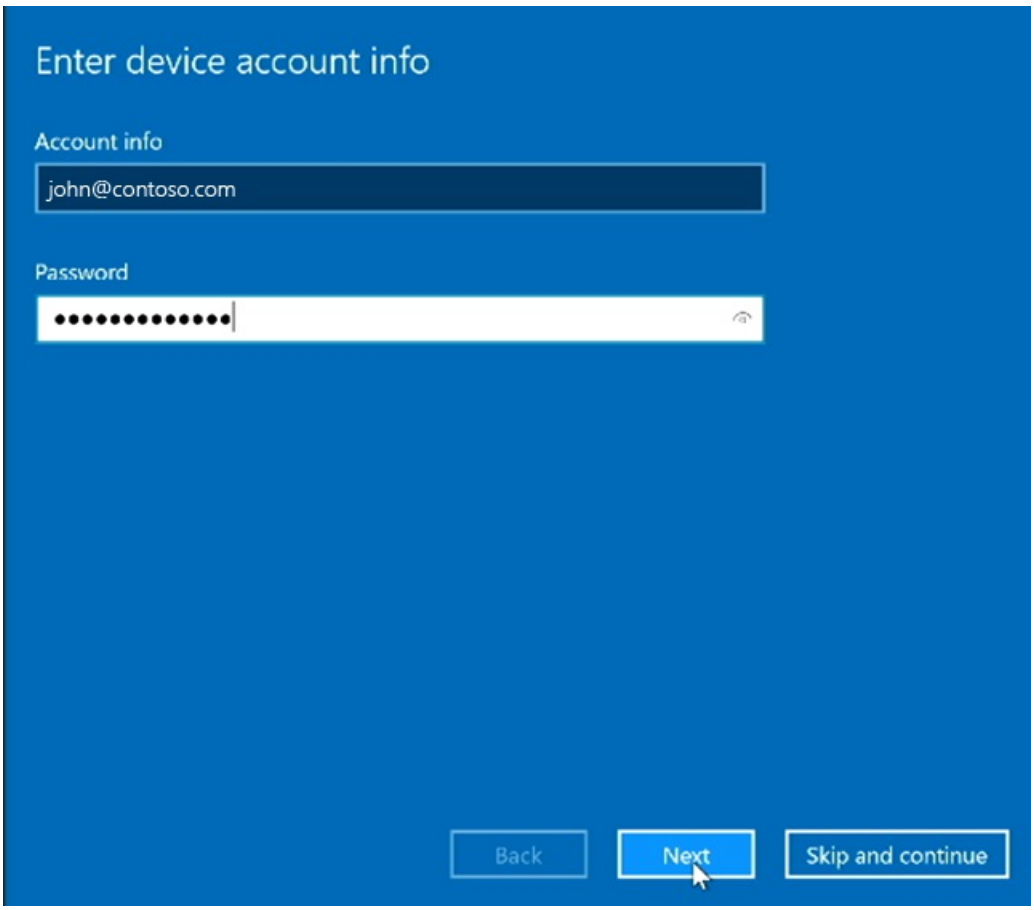
5. **Conectar a una red.** Si ya ha conectado un cable Ethernet, Surface Hub conectará automáticamente a la red. Como alternativa, puede conectarse a una red inalámbrica. **Nota:** No puede conectarse a una red inalámbrica en puntos de acceso (portales cautivos) que redirijan las solicitudes de inicio de sesión al sitio web de un proveedor. Selecciona **Siguiente**.



6. **Acepte Windows 10 de licencia.** Seleccione **Aceptar**.



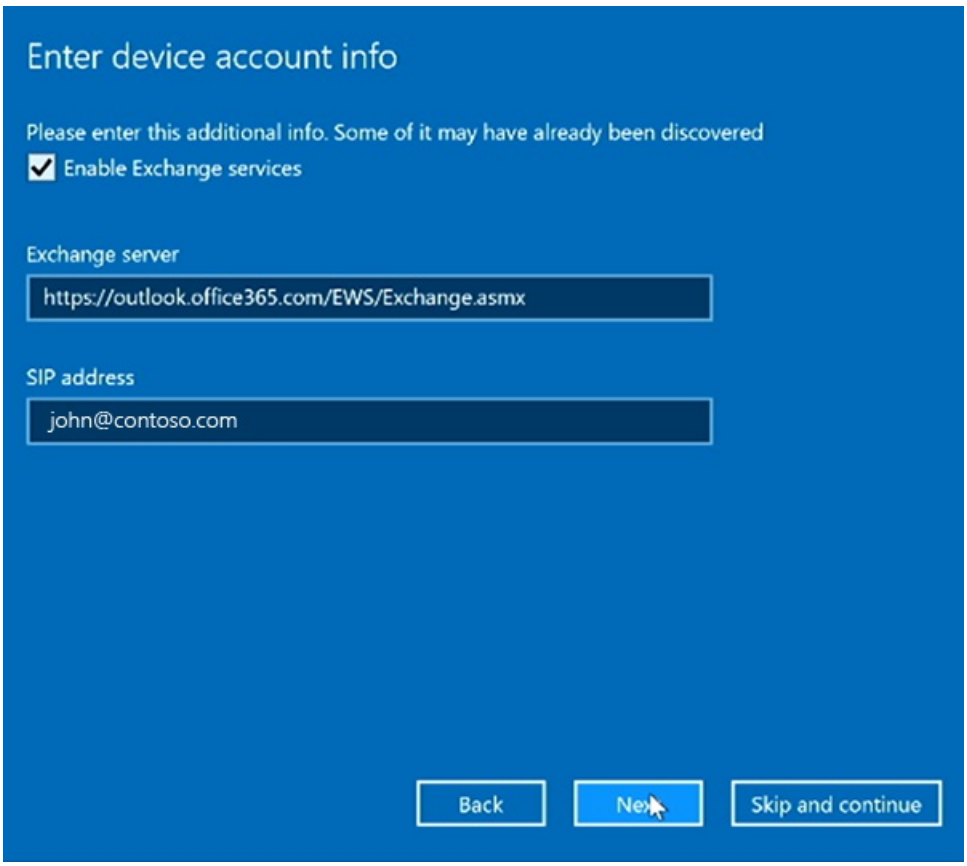
7. **Escribe información de cuenta de** dispositivo con una dirección UPN (user@contoso.com) o una dirección de dominio de nivel inferior (CONTOSO\usuario). Use el formato que coincida con el entorno y escriba la contraseña.



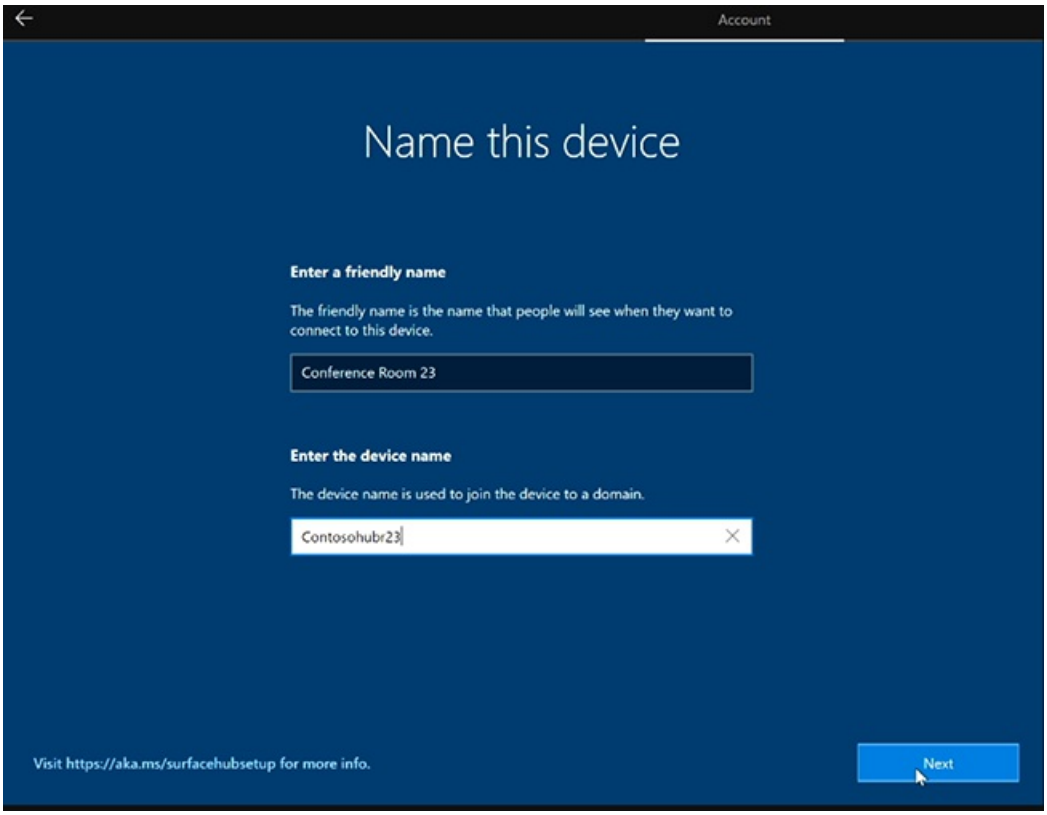
ENTORNO	FORMATO REQUERIDO PARA LA CUENTA DEL DISPOSITIVO
La cuenta de dispositivo se hospeda solo en línea	username@contoso.com
La cuenta de dispositivo solo se hospeda localmente	CONTOSO\user
La cuenta de dispositivo se hospeda en línea y local (híbrida)	CONTOSO\user

> **NOTE**
> Aunque puedes omitir la configuración de una cuenta de dispositivo, el dispositivo no estará totalmente integrado en la infraestructura. Si omites la configuración ahora, puedes agregar una cuenta del dispositivo más adelante mediante la aplicación Configuración.

8. **Escribe la contraseña y** selecciona **Siguiente.**
9. Surface Hub detecta automáticamente la información Exchange servidor y la dirección SIP del dominio especificado en el paso anterior. O, si es necesario, proporcione la dirección Exchange servidor y seleccione **Siguiente**.



10. **Asigne un nombre a este dispositivo.** Escribe un nombre para el dispositivo o usa el sugerido. **Seleccione Siguiente**.



- El **nombre descriptivo** está visible en la esquina inferior izquierda de Surface Hub 2S y se muestra al proyectar al dispositivo.
- El **nombre del dispositivo** identifica el dispositivo cuando está asociado con Active Directory o Azure Active Directory y al inscribir el dispositivo con Intune.

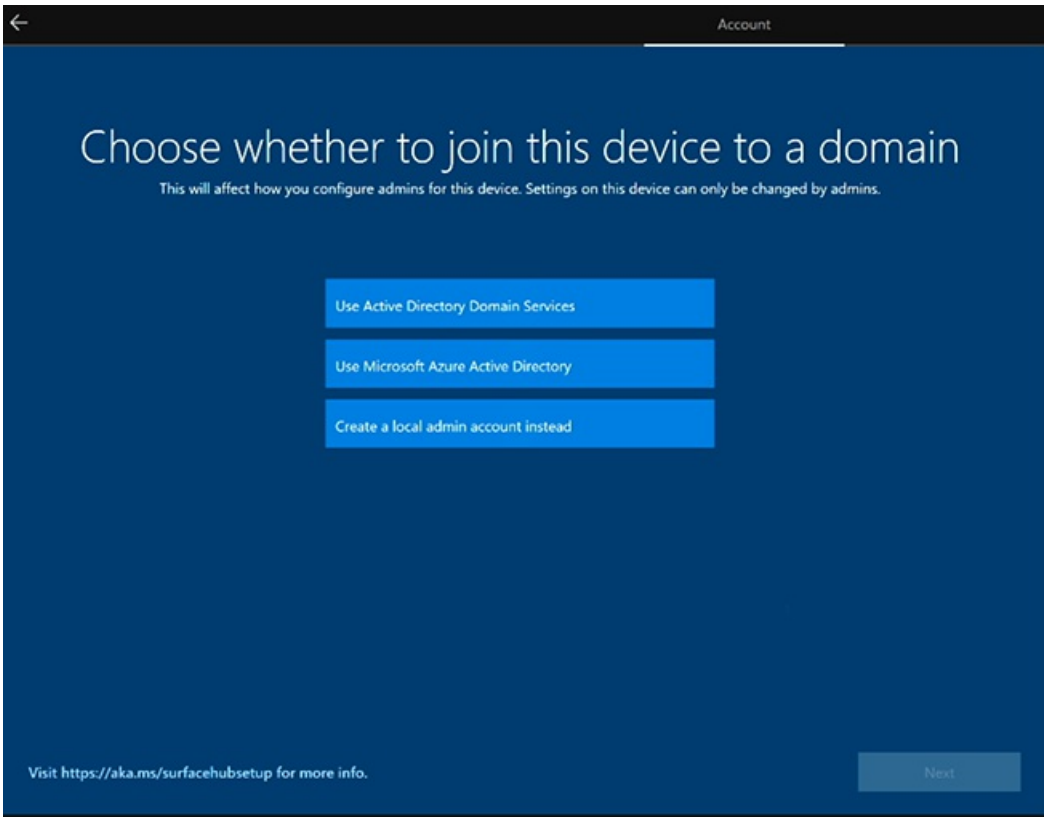
> **NOTE**
> Si quieres habilitar Miracast sobre infraestructura, el nombre del dispositivo debe ser reconocible mediante DNS. Puedes lograrlo permitiendo que Surface Hub se registre automáticamente a través de DNS dinámico, o crear manualmente un registro A o AAAA para el nombre de host del dispositivo Surface Hub.

Configurar cuentas de administrador de dispositivos

Solo puedes configurar administradores de dispositivos durante la configuración por primera vez. Para más información, consulta:

- Surface Hub de dispositivos 2S
- Administración del grupo de administradores

1. **Elija el tipo de cuenta de administrador.** Seleccione una de las siguientes opciones: Servicios de dominio de Active Directory, Azure Active Directory o Administrador local.



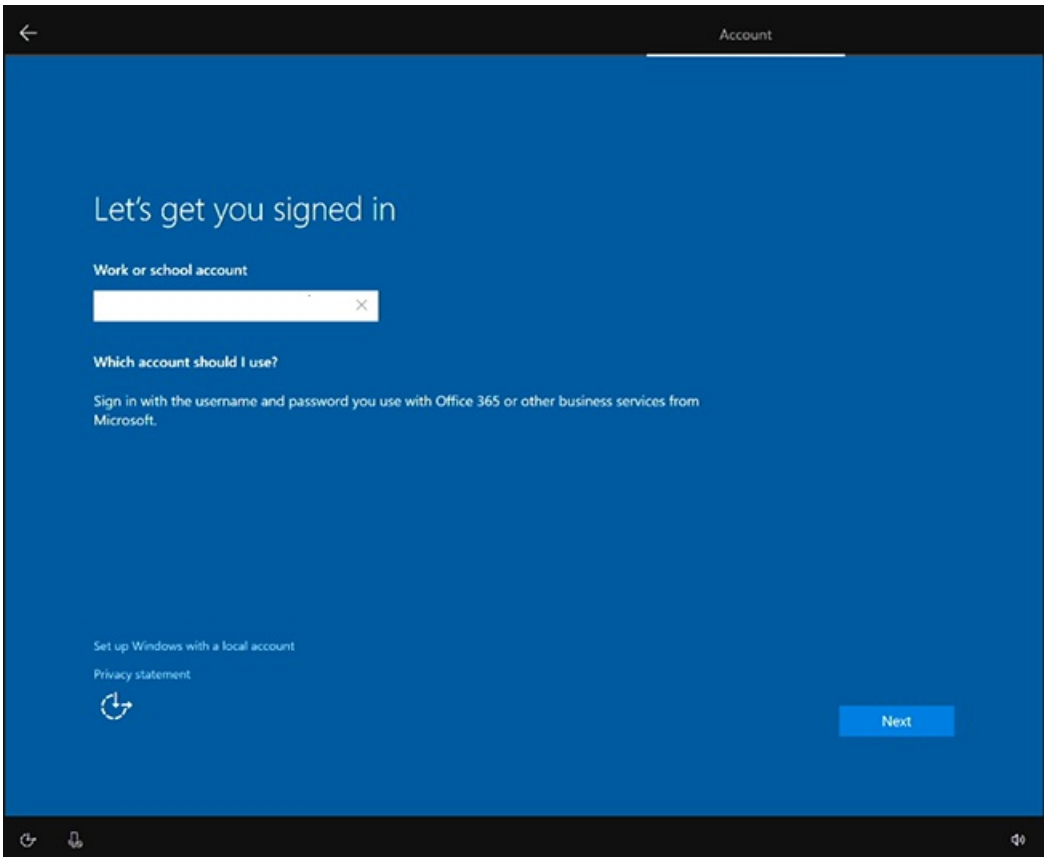
Active Directory Domain Services

1. Si tiene la intención de usar Surface Hub en un entorno local, puede asociar El concentrador con **los servicios de dominio de Active Directory**. Escriba las credenciales de un usuario que tenga permisos para unirse al dispositivo a Active Directory.
2. Selecciona el grupo de seguridad de Active Directory que contiene los miembros que pueden iniciar sesión en la Configuración en Surface Hub 2S.
3. Seleccione **Finalizar**. El dispositivo se reiniciará.

Microsoft Azure Active Directory

1. Si tienes la intención de administrar Surface Hub desde la nube con Microsoft Intune o un proveedor MDM, selecciona **Microsoft Azure Active Directory**.

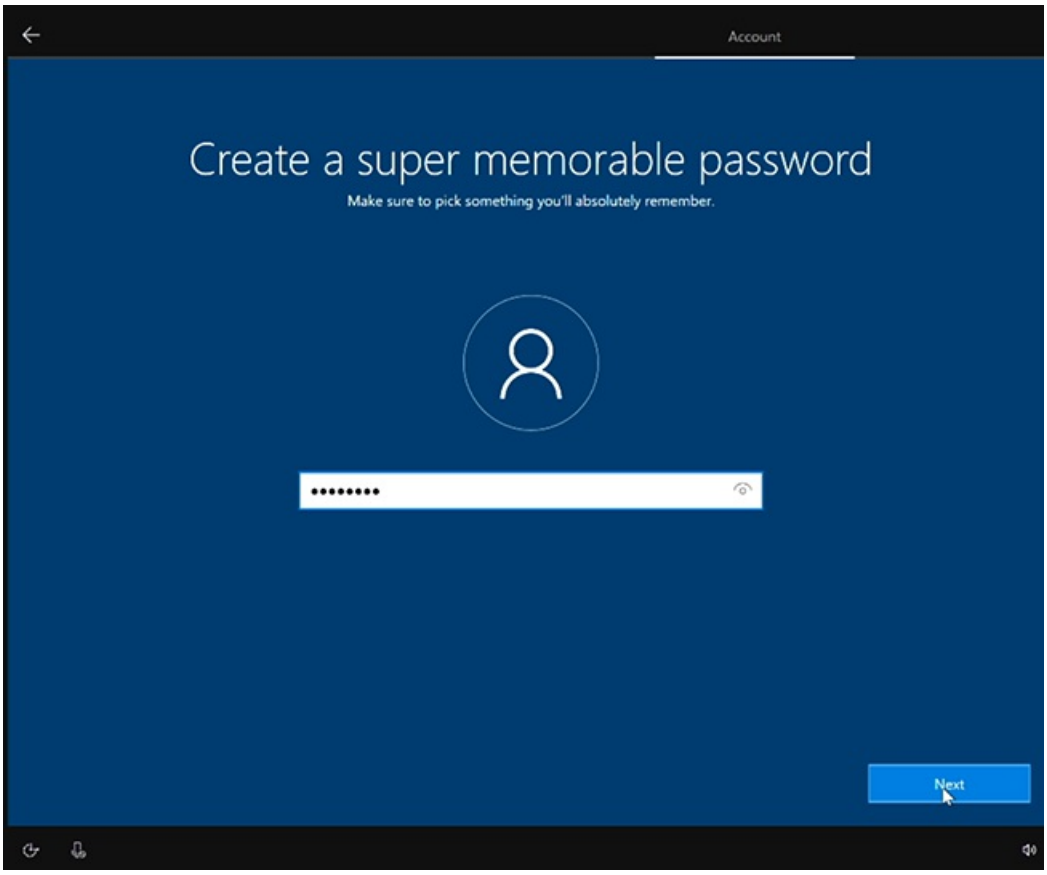
2. Seleccione Siguiente e inicie sesión con una cuenta laboral o educativa. Si se redirige, autentique con la página de inicio de sesión de su organización y proporcione credenciales adicionales si se solicita. De lo contrario, escriba la contraseña y seleccione **Siguiente.**



> **NOTE**
> Para configurar quién puede usar la aplicación Configuración para administrar Surface Hubs, asegúrese de que la inscripción automática de Intune está habilitada en el inquilino antes de unir el dispositivo a Azure AD. Las directivas de Intune se pueden usar para configurar administradores que no son globales en Surface Hubs.

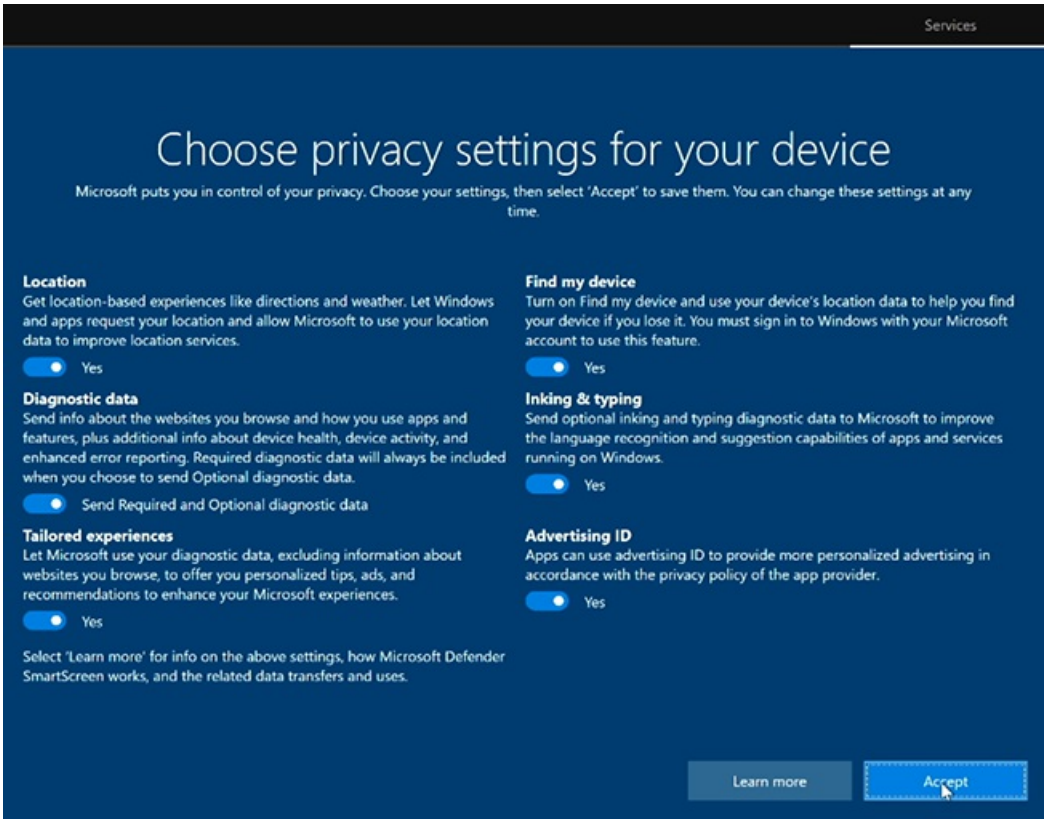
Cuenta de administrador local

- Escriba un nombre de usuario y una contraseña memorable para el administrador local. (Si olvida la contraseña de administrador local, tendrá que recuperar el dispositivo y repetir el proceso de configuración).



Elegir la configuración de privacidad del dispositivo

- Seleccione entre la configuración de privacidad disponible y seleccione **Aceptar.**



Usar paquetes de aprovisionamiento

Puedes personalizar las opciones de configuración por primera vez, lo que te permite garantizar una experiencia coherente en varios Surface Hubs.

1. Para empezar, revise la documentación de Crear paquetes de aprovisionamiento y guarde el paquete de aprovisionamiento en una unidad usb.

2. Inserte la unidad usb en uno de los puertos USB antes de iniciar el proceso de configuración.
3. Cuando se le pida, elija el paquete de aprovisionamiento que desea usar.
4. Si creaste un archivo CSV de varios dispositivos, podrás elegir una configuración de dispositivo.
5. Siga las instrucciones para completar el programa de instalación por primera vez.

Administración de grupos de administración para Surface Hub

12/01/2022 • 4 minutes to read

Cada Surface Hub se puede configurar localmente mediante la aplicación Configuración en el dispositivo. Para impedir que usuarios no autorizados cambien la configuración, la aplicación Configuración requiere credenciales de administrador para abrir la aplicación.

Administración del grupo de administradores

Puedes configurar cuentas de administrador para el dispositivo de las siguientes maneras:

- Crear una cuenta de administrador local
- Unir el dispositivo a Active Directory
- Azure AD unirse al dispositivo
- Configurar cuentas de administrador no globales en Azure AD unidos (Surface Hub 2S)

Crear una cuenta de administrador local

Para crear un administrador local, elige usar un administrador local durante la primera ejecución. De este modo, se creará una cuenta de administrador local única en Surface Hub con el nombre de usuario y la contraseña de tu elección. Usa estas credenciales para abrir la aplicación Configuración.

Ten en cuenta que la información de cuenta de administrador local no está respaldada por ningún servicio de directorio. Te recomendamos que elijas solo un administrador local si el dispositivo no tiene acceso a Active Directory (AD) o Azure Active Directory (Azure AD). Si decides cambiar la contraseña del administrador local, puedes hacerlo en Configuración. Sin embargo, si quieres cambiar de una cuenta de administrador local a un grupo de tu dominio o inquilino de Azure AD, tendrás que restablecer el dispositivo y volver a ejecutar el programa como la primera vez.

Unir el dispositivo a Active Directory

Puedes unir Surface Hub a tu dominio de AD para permitir que los usuarios de un grupo de seguridad especificado puedan configurar los parámetros. Durante la primera ejecución, elige usar los servicios de dominio de Active Directory. Deberás proporcionar las credenciales que son capaces de unir el dominio de tu elección y el nombre de un grupo de seguridad existente. Cualquier persona que sea miembro de ese grupo de seguridad puede escribir sus credenciales y desbloquear Configuración.

¿Qué sucede cuando unes tu Surface Hub a un dominio?

Los Surface Hubs usan unión a un dominio para:

- Conceder derechos de administrador a los miembros de un grupo de seguridad especificado en AD.
- Copia de seguridad de la clave de recuperación de BitLocker del dispositivo, almacenándola en el objeto del equipo en AD. Consulta Guardar la clave de BitLocker para obtener más información.
- Sincronizar el reloj del sistema con el controlador de dominio para la comunicación cifrada

Surface Hub no admite la aplicación de directivas de grupo o certificados desde el controlador de dominio.

> **NOTE**
> Si el Surface Hub pierde confianza en el dominio (por ejemplo, si se quita el Surface Hub del dominio cuando esté unido a este), no podrás autenticarte en el dispositivo ni abrir Configuración. Si decides quitar la relación de confianza entre el Surface Hub y tu dominio, restablece el dispositivo en primer lugar.

Azure AD unirse al dispositivo

Puede Azure Active Directory (Azure AD) unirse a la Surface Hub para permitir que los profesionales de TI de su inquilino Azure AD configurar la configuración. Durante la primera ejecución, elige usar Microsoft Azure Active Directory. Deberás proporcionar las credenciales que se pueden unir al inquilino de Azure AD de tu elección. Después de unirte a Azure AD correctamente, se concederán los derechos de administrador a las personas adecuadas en el dispositivo.

De manera predeterminada, se concederán derechos de administrador a todos los **administradores globales** en un Surface Hub unido a Azure AD. Con **Azure AD Premium** o **Enterprise Mobility Suite (EMS)**, puedes agregar administradores adicionales:

1. En el portal de Azure clásico, haz clic en **Active Directory** y, a continuación, haz clic en el nombre del directorio de la organización.
2. En la página **Configurar**, en **Dispositivos** > **Administradores adicionales en los dispositivos unidos a Azure AD**, haz clic en **Seleccionados**.
3. Haz clic en **Agregar** y selecciona los usuarios que quieres agregar como administradores en tu Surface Hub y en otros dispositivos unidos a Azure AD.
4. Cuando hayas terminado, haz clic en el botón de marca de verificación para guardar el cambio.

¿Qué sucede al unir el Surface Hub a Azure AD?

Los Surface Hubs usan la unión a Azure AD para:

- Conceder derechos de administrador a los usuarios adecuados en el inquilino de Azure AD.
- Copia de seguridad de la clave de recuperación de BitLocker del dispositivo, almacenándola en la cuenta que se usó para unir el dispositivo a Azure AD. Consulta Guardar la clave de BitLocker para obtener más información.

Inscripción automática a través Azure Active Directory unirse

Surface Hub ahora admite la capacidad de inscribirse automáticamente en Intune uniendo el dispositivo a Azure Active Directory.

Para obtener más información, vea Enable Windows 10 automatic enrollment.

¿Cuál debo elegir?

Si tu organización usa AD o Azure AD, te recomendamos que te unas a un dominio o a Azure AD, principalmente por motivos de seguridad. Las personas podrán autenticarse y desbloquear Configuración con sus propias credenciales y se pueden mover dentro o fuera de los grupos de seguridad asociados a tu dominio.

OPCIÓN	REQUISITOS	¿QUÉ CREDENCIALES SE PUEDEN USAR PARA ACCEDER A LA APLICACIÓN CONFIGURACIÓN?
Crear una cuenta de administrador local	Ninguna	El nombre de usuario y contraseña especificados durante la primera ejecución
Unión a un dominio de Active Directory (AD)	Tu organización usa AD	Cualquier usuario de AD de un grupo de seguridad específico de tu dominio

OPCIÓN	REQUISITOS	¿QUÉ CREDENCIALES SE PUEDEN USAR PARA ACCEDER A LA APLICACIÓN CONFIGURACIÓN?
Unir el dispositivo a Azure Active Directory (Azure AD)	Tu organización usa Azure AD Basic	Solo los administradores globales
	Tu organización usa Azure AD Premium o Enterprise Mobility Suite (EMS)	Los administradores globales y los administradores adicionales

Configurar cuentas de administración no globales en Azure AD dispositivos unidos

Para Surface Hub v1 y Surface Hub dispositivos 2S unidos a Azure AD, Windows 10 Team 2020 Update te permite limitar los permisos de administrador a la administración de la aplicación Configuración en Surface Hub. Esto le permite tener en cuenta los permisos de administración Surface Hub y evitar el acceso de administrador potencialmente no deseado a un dominio Azure AD usuario. Para obtener más información, vea Configure non Global admin accounts on Surface Hub.

Crear y probar una cuenta del dispositivo (Surface Hub)

12/01/2022 • 4 minutes to read

La creación de una cuenta de dispositivo Surface Hub (también conocida como cuenta de recurso/buzón de sala) permite al Surface Hub recibir, aprobar o rechazar solicitudes de reunión y unirse a reuniones.

Una vez que la cuenta del dispositivo se aprovisiona en un Surface Hub, los usuarios pueden agregar esta cuenta a una invitación a una reunión del mismo modo que invitarían a una sala de conferencias.

Puedes configurar la cuenta del dispositivo durante la configuración de la experiencia de salida (OOBE). Si es necesario, también puede cambiarlo más adelante **en Configuración** > **Surface Hub** > **Accounts**.

Introducción a la configuración

Esta tabla explica los pasos principales y las decisiones de configuración cuando se crea una cuenta del dispositivo.

PASO	DESCRIPCIÓN	PROPÓSITO
1	Crear un buzón de sala habilitado para inicio de sesión (Exchange Online o Exchange Server 2016 y versiones posteriores)	Este tipo de buzón permite al dispositivo mantener un calendario de reuniones, recibir solicitudes de reunión y enviar correo. Debe estar habilitado para el inicio de sesión para poder usarse con un Surface Hub.
2	Configurar las propiedades de buzón de correo	El buzón de correo debe estar configurado con las propiedades correctas para obtener la mejor experiencia de reunión en Surface Hub. Para obtener más información acerca de las propiedades del buzón de correo, consulta Propiedades del buzón.
3	Asegúrese de Exchange web Services (EWS) está habilitado y de que la autenticación multifactor (MFA) está deshabilitada	El Surface Hub usa EWS para sincronizar su calendario. Si no permite EWS en el entorno de forma predeterminada, el buzón de concentradores tendría que tenerla habilitada explícitamente. Como el Surface Hub inicia sesión Exchange en segundo plano sin la interacción del usuario, no puede responder a ningún mensaje interactivo, como MFA. La cuenta de dispositivo que cree debe excluirse de dichos requisitos de autenticación. De lo contrario, Surface Hub no podrá sincronizar el correo ni la información de calendario.

PASO	DESCRIPCIÓN	PROPÓSITO
4	Habilitar la cuenta para Teams o Skype Empresarial (Skype Empresarial Server 2015 y versiones posteriores)	Skype Empresarial o Teams deben habilitarse para usar características de conferencia como videollamadas y uso compartido de pantalla. Para obtener más información sobre las licencias que Teams, vea Teams Sala de reuniones licensing and Teams service description. Las aplicaciones Teams y SfB de la Surface Hub no son compatibles con las directivas de acceso condicional de Azure AD que requieren información del dispositivo (por ejemplo, cumplimiento). La cuenta de dispositivo que cree debe excluirse de dichas directivas de CA. De lo contrario, Surface Hub no puede usar ninguna función de conferencia.
5	(Opcional) Deshabilitar la caducidad de contraseña	Para simplificar la administración, puedes desactivar la caducidad de contraseña para la cuenta del dispositivo y permitir que Surface Hub rote automáticamente la contraseña de la cuenta del dispositivo. Para obtener más información acerca de la administración de contraseñas, consulta Administración de contraseñas.
6	(Opcional) Configurar Exchange directivas para permitir ActiveSync	Con determinadas implementaciones Exchange Server & de Active Directory locales, ActiveSync se usará para sincronizar el correo de la cuenta del dispositivo y la información del calendario. Para obtener más información acerca de las directivas que se configurarán, vea Directivas de ActiveSync para Surface Hub cuentas.

NOTE

La Surface Hub de dispositivo no admite proveedores de identidades federados (IDP) de terceros y debe autenticarse a través de Active Directory o Azure Active Directory.

Pasos detallados de la configuración

Se recomienda configurar las cuentas Surface Hub dispositivo mediante el uso de Windows PowerShell. Microsoft proporciona SkypeRoomProvisioningScript.ps1, un script que ayudará a crear nuevas cuentas de recursos o validar cuentas de recursos existentes que tenga para ayudarle a convertirlos en cuentas de dispositivo Surface Hub compatibles. Si lo prefiere, puede elegir una opción de la tabla siguiente y seguir los pasos detallados de PowerShell en función de la implementación de la organización.

IMPLEMENTACIÓN DE LA ORGANIZACIÓN	DESCRIPCIÓN	FORMATO QUE SE USARÁ DURANTE SURFACE HUB INSTALACIÓN
Implementación en línea (Microsoft 365 o Office 365)	El entorno de la organización se implementa completamente en Microsoft 365 o Office 365.	nombreusuario@dominio.com
Implementación híbrida (Exchange local)	Su organización tiene una combinación de servicios, con Exchange Server local y Microsoft Teams en línea.	username@domain.com si la autenticación moderna híbrida está habilitada en Exchange, DOMAIN\username en caso contrario
Implementación híbrida (Exchange Online)	Su organización tiene una combinación de servicios, con Skype Empresarial Server local y Exchange Online.	username@domain.com si la autenticación moderna híbrida está habilitada en SfB, DOMAIN\username de lo contrario
Implementación local (bosque único)	Su organización tiene servidores que controla, donde Active Directory, Exchange y Skype Empresarial Server se hospedan en un entorno de bosque único.	DOMINIO\nombre de usuario
Implementación local (varios bosques)	Su organización tiene servidores que controla, donde Active Directory, Exchange y Skype Empresarial Server se hospedan en un entorno de varios bosques.	ACCOUNTFOREST\username

Verificación y prueba de cuentas

Hay dos métodos disponibles que puedes usar para validar y probar una cuenta Surface Hub dispositivo:SkypeRoomProvisioningScript.ps1y la aplicación Surface Hub de diagnóstico de hardware. El script de aprovisionamiento de cuenta puede validar una cuenta de dispositivo creada previamente con PowerShell desde el equipo. La aplicación Diagnóstico de hardware de Surface Hub se instala en Surface Hub y proporciona información detallada acerca de los errores de inicio de sesión y comunicación. Ambas son herramientas valiosas para probar las cuentas del dispositivo recién creadas y deben usarse para garantizar una óptima disponibilidad de las cuentas.

Propiedades de Microsoft Exchange (Surface Hub)

12/01/2022 • 2 minutes to read

Algunas propiedades de Microsoft Exchange de la cuenta del dispositivo se deben establecer en determinados valores para obtener la mejor experiencia de reunión en Microsoft Surface Hub. La siguiente tabla enumera varias propiedades de Exchange basadas en parámetros de cmdlet de PowerShell, su propósito y los valores en los que se deberían establecer.

PROPIEDAD	DESCRIPCIÓN	VALOR	IMPACTO
AutomateProcessing	El parámetro AutomateProcessing habilita o deshabilita el procesamiento de calendario en el buzón.	AutoAccept	El Surface Hub podrá aceptar o rechazar automáticamente las convocatorias de reunión según su disponibilidad.
AddOrganizerToSubject	El parámetro AddOrganizerToSubject especifica si el nombre del organizador de la reunión se usa como el asunto de la convocatoria de reunión.	$False	La pantalla de bienvenida no mostrará al organizador de la reunión dos veces (en lugar de mostrarlo tanto como el organizador como el asunto de la reunión).
AllowConflicts	El parámetro AllowConflicts especifica si se permiten convocatorias de reunión en conflicto.	$False	El Surface Hub rechazará las convocatorias de reunión que entren en conflicto con la hora de otra reunión.
DeleteComments	El parámetro DeleteComments especifica si se quita o se mantiene cualquier texto en el cuerpo del mensaje de las convocatorias de reunión entrantes.	$False	El cuerpo del mensaje de las reuniones se puede conservar y recuperar desde un Surface Hub si lo necesitas durante una reunión.
DeleteSubject	El parámetro DeleteSubject especifica si se debe quitar o mantener el asunto de las convocatorias de reunión entrantes.	$False	Los temas de las convocatorias de reunión se puede mostrar en el Surface Hub.

PROPIEDAD	DESCRIPCIÓN	VALOR	IMPACTO
RemovePrivateProperty	El parámetro RemovePrivateProperty especifica si se borra la marca privada para las convocatorias de reunión entrantes.	$False	Los temas de las reuniones privadas se mostrará como Privado en la pantalla de bienvenida.
AddAdditionalResponse	El parámetro AddAdditionalResponse especifica si se enviará información adicional desde el buzón de recursos al responder a las convocatorias de reunión.	$True	Cuando se envía una respuesta a una convocatoria de reunión, se proporcionará texto personalizado en la respuesta.
AdditionalResponse	El parámetro AdditionalResponse especifica la información adicional que se incluirá en las respuestas a las convocatorias de reunión. **Nota:** este texto no se enviará a menos que AddAdditionalResponse se establezca en $true.	Tu elección: la respuesta adicional se puede usar para indicar a los usuarios cómo usar un Surface Hub o guiarlos a los recursos.	Al añadir un mensaje de respuesta adicional se puede proporcionar a los usuarios una introducción sobre cómo pueden usar un Surface Hub en su reunión.

Aplicación de directivas de ActiveSync a las cuentas de dispositivo (Surface Hub)

12/01/2022 • 2 minutes to read

Los Surface Hub que usan cuentas de dispositivo **** de Active Directory (aprovisionadas en el concentrador en formato dominio\nombredeusuario) y los servicios de Exchange locales usan ActiveSync para sincronizar el correo y el calendario. Esto permite a los usuarios unirse e iniciar reuniones programadas desde Surface Hub, así como enviar por correo electrónico cualquier pizarra interactiva realizada durante la reunión.

Para que estas características funcionen, las directivas de ActiveSync de tu organización deben configurarse de la siguiente manera:

- No puede haber ninguna directiva global que bloquee la sincronización del buzón de recursos que está usando la cuenta del dispositivo de Surface Hub. Si hay una directiva de bloqueo de este tipo, debes agregar Surface Hub como dispositivo permitido.
- Debes establecer una directiva de buzón de dispositivo móvil donde la **PasswordEnabled** configuración esté establecida en False. Otras opciones de configuración de directiva de buzón de dispositivo móvil no son compatibles con el Surface Hub.

Permitir deviceid

La organización puede tener una directiva global que impida la sincronización de cuentas de dispositivos aprovisionadas en Surface Hubs. Para configurar esta propiedad, consulta Permitir id. de dispositivo para ActiveSync.

Configuración PasswordEnabled

La cuenta del dispositivo debe tener una directiva ActiveSync donde el atributo **PasswordEnabled** esté establecido en False o 0. Para configurar esta propiedad, consulta Creación de una directiva de Microsoft Exchange ActiveSync compatible con Surface Hub.

Crear paquetes de aprovisionamiento para Surface Hub

12/01/2022 • 13 minutes to read

Los paquetes de aprovisionamiento te permiten automatizar la implementación de características clave, lo que ayuda a ofrecer una experiencia coherente en todos los Surface Hubs de tu organización. Con Windows Configuration Designer (WCD) en un equipo independiente, puede completar las siguientes tareas:

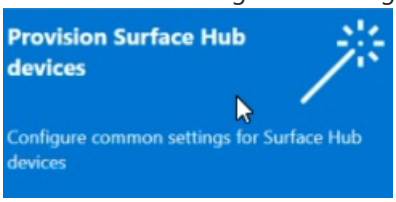
- Inscribirse en Active Directory o Azure Active Directory
- Crear una cuenta de administrador de dispositivos
- Agregar aplicaciones y certificados
- Definir la configuración de proxy
- Agregar un archivo de configuración de Surface Hub
- Configurar la configuración del proveedor de servicios de configuración (CSP)

Introducción

1. En un equipo independiente que ejecute Windows 10, instale Windows Configuration Designer desde el Microsoft Store.
2. Selecciona **Aprovisionar Surface Hub dispositivos para** configurar opciones comunes mediante un asistente. O bien, seleccione Aprovisionamiento avanzado para ver y configurar todas las opciones posibles.
3. Cree el paquete de aprovisionamiento y guárdelo en una unidad USB.
4. Implemente el paquete en su Surface Hub durante la instalación de la primera ejecución o a través de la Configuración aplicación. Para obtener más información, vea Create a provisioning package for Windows 10.

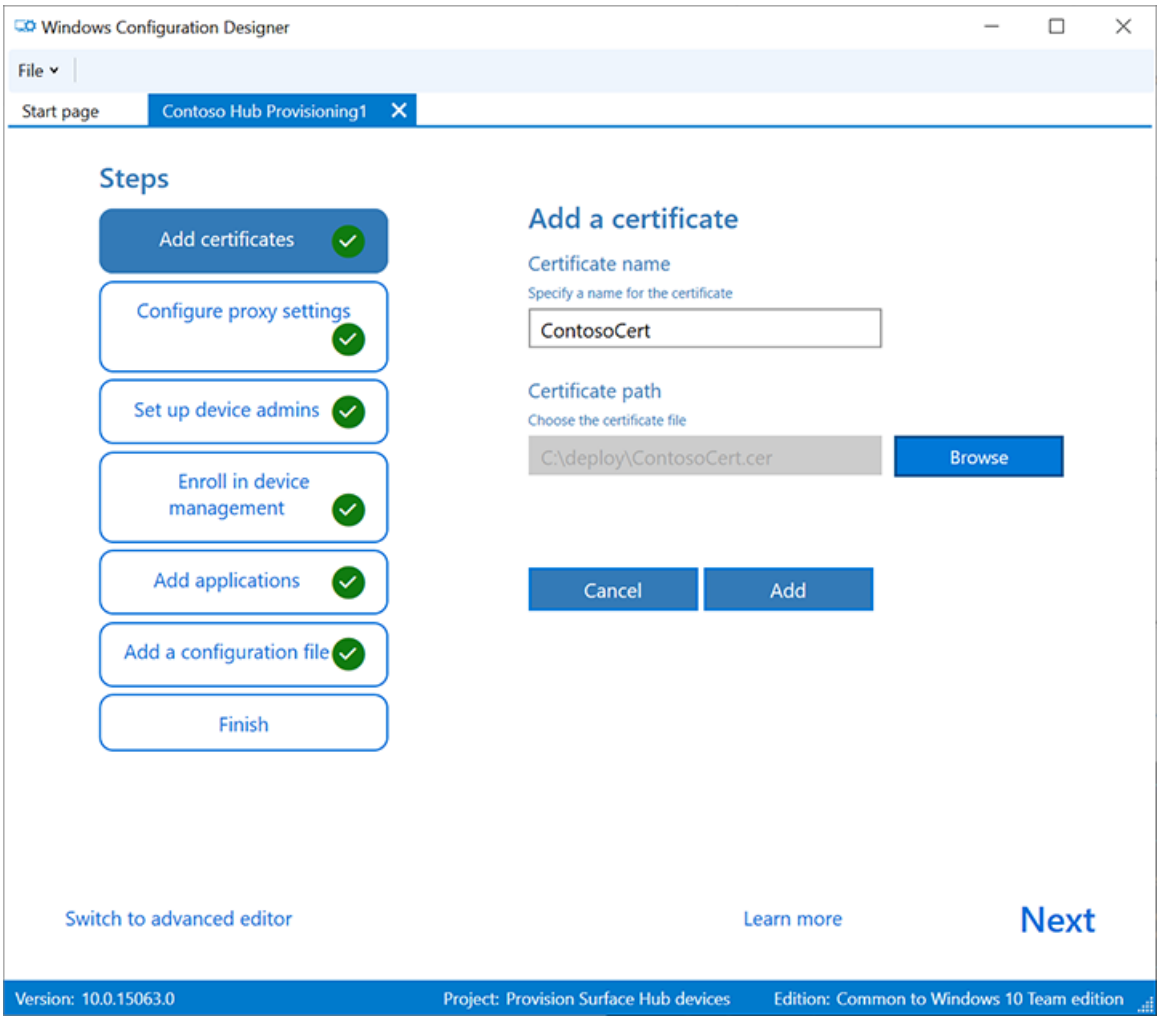
Usar Surface Hub de aprovisionamiento

1. Abra Windows Configuration Designer y seleccione **Aprovisionar Surface Hub dispositivos**.



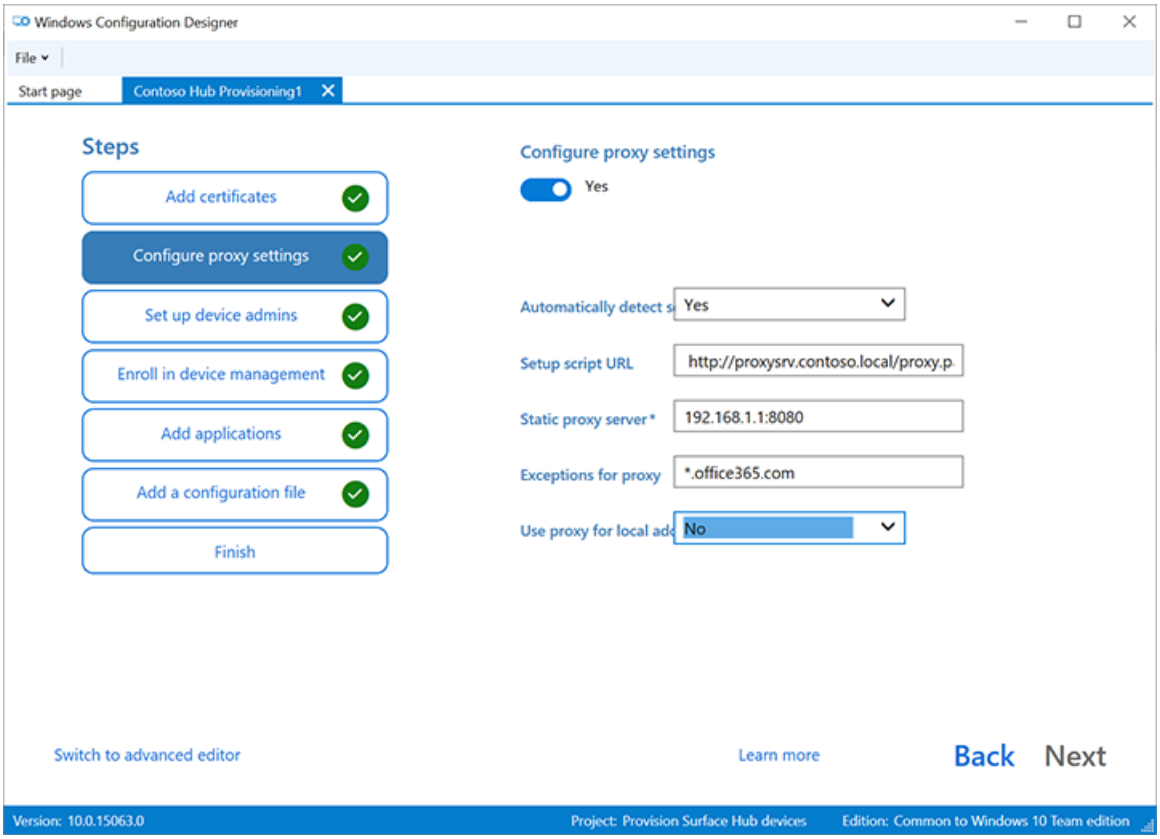
2. Asigne un nombre al proyecto y seleccione **Siguiente**.

Agregar certificados



Para aprovisionar el dispositivo con un certificado, **seleccione Agregar un certificado**. Escriba un nombre para el certificado y, a continuación, busque para seleccionar el certificado que se va a usar. Para obtener opciones avanzadas de aprovisionamiento, consulte la sección siguiente Agregar un certificado al paquete.

Definir la configuración de proxy



1. Alterna **Sí** o **No** para la configuración de proxy. De forma predeterminada, Surface Hub automáticamente detecta la configuración de proxy. Sin embargo, si anteriormente tu infraestructura requería el uso de un servidor proxy y ahora ha cambiado y ya no lo requiere, puedes usar un paquete de aprovisionamiento para revertir los dispositivos Surface Hub a la configuración predeterminada seleccionando **Sí** y **Detectar la configuración automáticamente**.

2. Si alterna **Sí**, puede seleccionar para detectar automáticamente la configuración de proxy o configurar manualmente la configuración especificando una de las siguientes opciones:

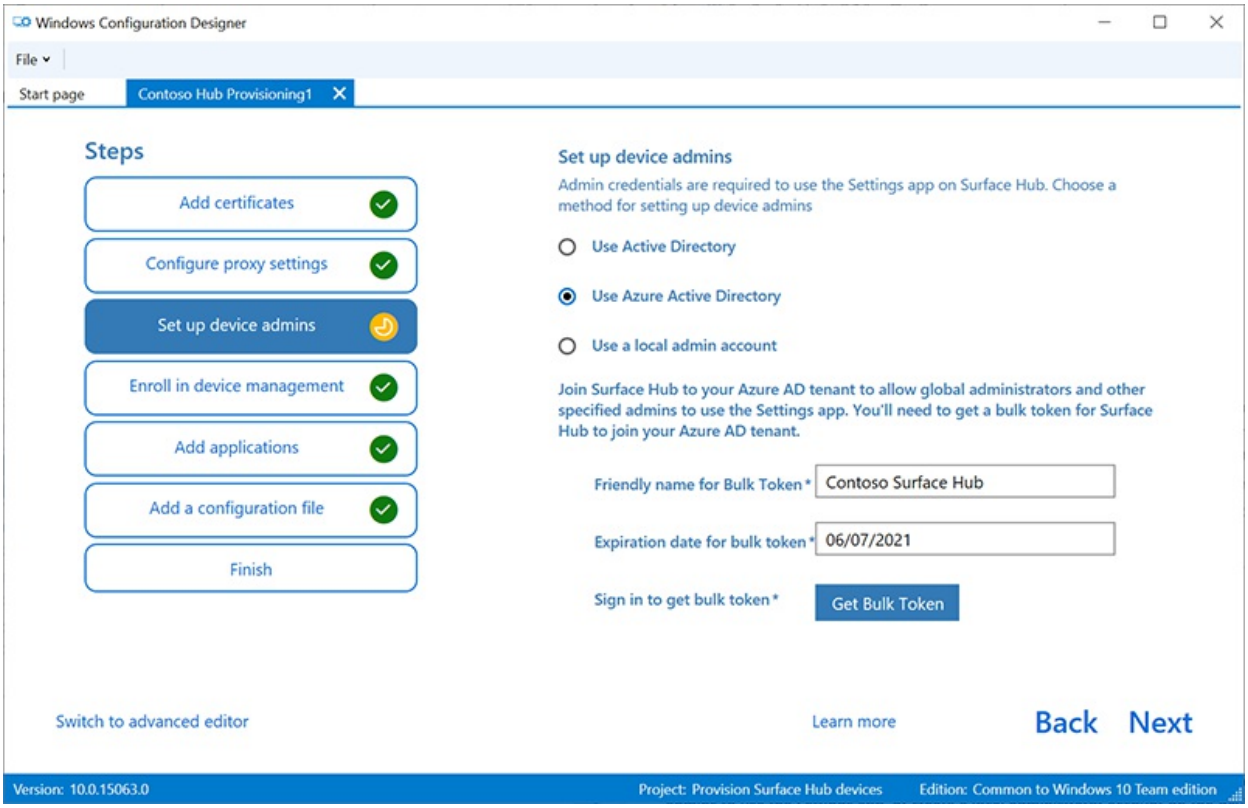
   - Dirección URL de un script de instalación.
   - Una dirección de servidor proxy estático e información de puerto.

3. Si desea usar un script de instalación o un servidor proxy, desactive **Detectar automáticamente la configuración**. Puede usar un script de instalación *o un* servidor proxy, no ambos.

4. Escriba excepciones (direcciones a las Surface Hub deben conectarse directamente sin usar el servidor proxy). **Ejemplo:** *.office365.com

5. Identificar si se va a usar el servidor proxy para las direcciones locales.

Configurar administradores de dispositivos



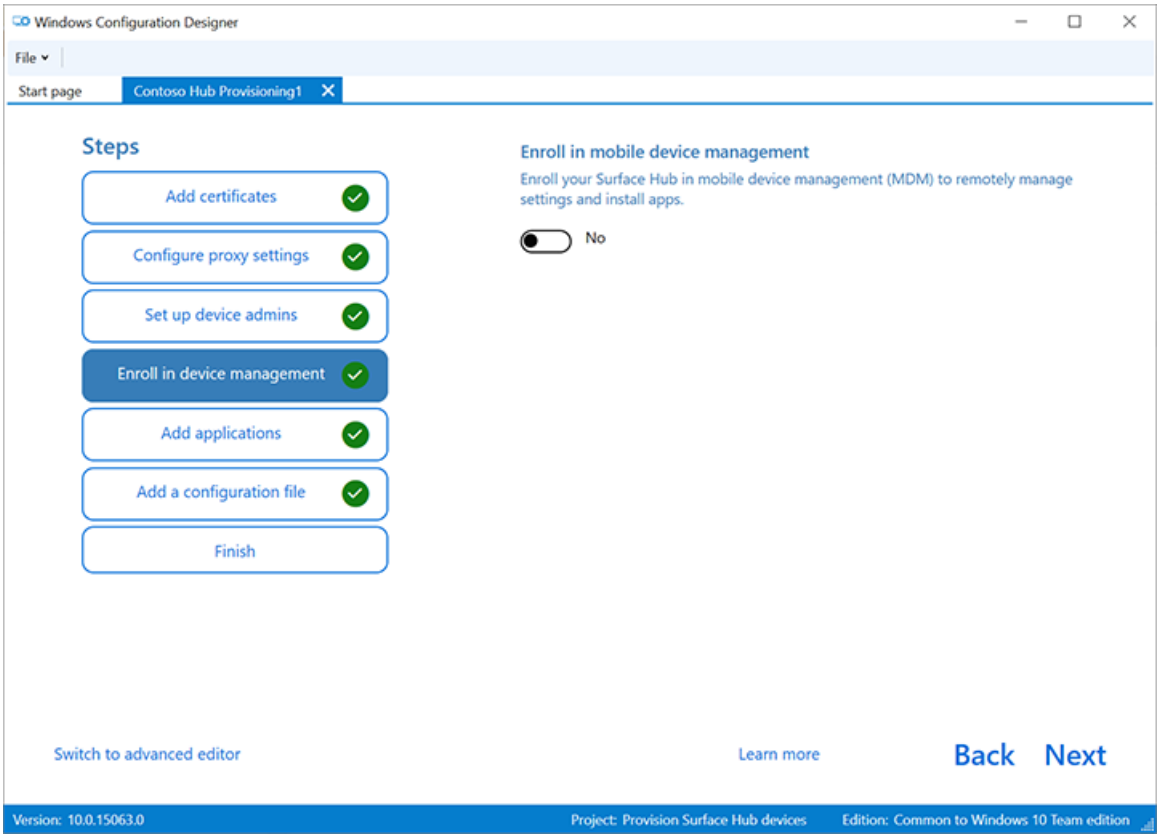
Puedes inscribir el dispositivo en Active Directory y especificar un grupo de seguridad para que use la aplicación Configuración, inscribirlo en Azure Active Directory para permitir que los administradores globales usen la aplicación Configuración o crear una cuenta de administrador local en el dispositivo.

1. Para inscribir el dispositivo en Active Directory, escribe las credenciales de una cuenta de usuario con privilegios mínimos para unir el equipo al dominio y especifica que el grupo de seguridad tenga credenciales de administrador en Surface Hub. Si aplica el paquete a un Surface Hub que se ha restablecido, puede usar la misma cuenta de dominio siempre que sea la misma cuenta la que configure el Surface Hub inicialmente. De lo contrario, se tiene que usar una cuenta de dominio diferente en el paquete de aprovisionamiento.
2. Antes de usar Windows Configuration Designer para configurar la inscripción masiva de Azure AD, planee laimplementación de la combinación de Azure AD . La opción **Número máximo de dispositivos por usuario** del inquilino de Azure AD determina cuántas veces se puede usar el token masivo que se obtiene en el asistente.

3. Para inscribir el dispositivo en Azure AD, selecciona esa opción y escribe un nombre descriptivo para el token masivo que obtendrás mediante el asistente. Establece una fecha de expiración del token (el máximo es de 30 días a partir de la fecha de obtención del token). Seleccione **Obtener token masivo**. En la ventana **Vamos a iniciar sesión**, escribe una cuenta que tenga permisos para unir un dispositivo a AzureAD y luego la contraseña. Seleccione **Aceptar** para conceder a Windows Configuration Designer los permisos necesarios.
4. Para crear una cuenta de administrador local, selecciona esa opción y escribe un nombre de usuario y una contraseña.

> **IMPORTANT**
>
> Si creas una cuenta local en el paquete de aprovisionamiento, debes cambiar la contraseña mediante la aplicación **Configuración** cada 42 días. Si la contraseña no se cambia en ese período, es posible que la cuenta se bloquee y no se pueda iniciar sesión.

Inscribirse en un proveedor MDM de terceros

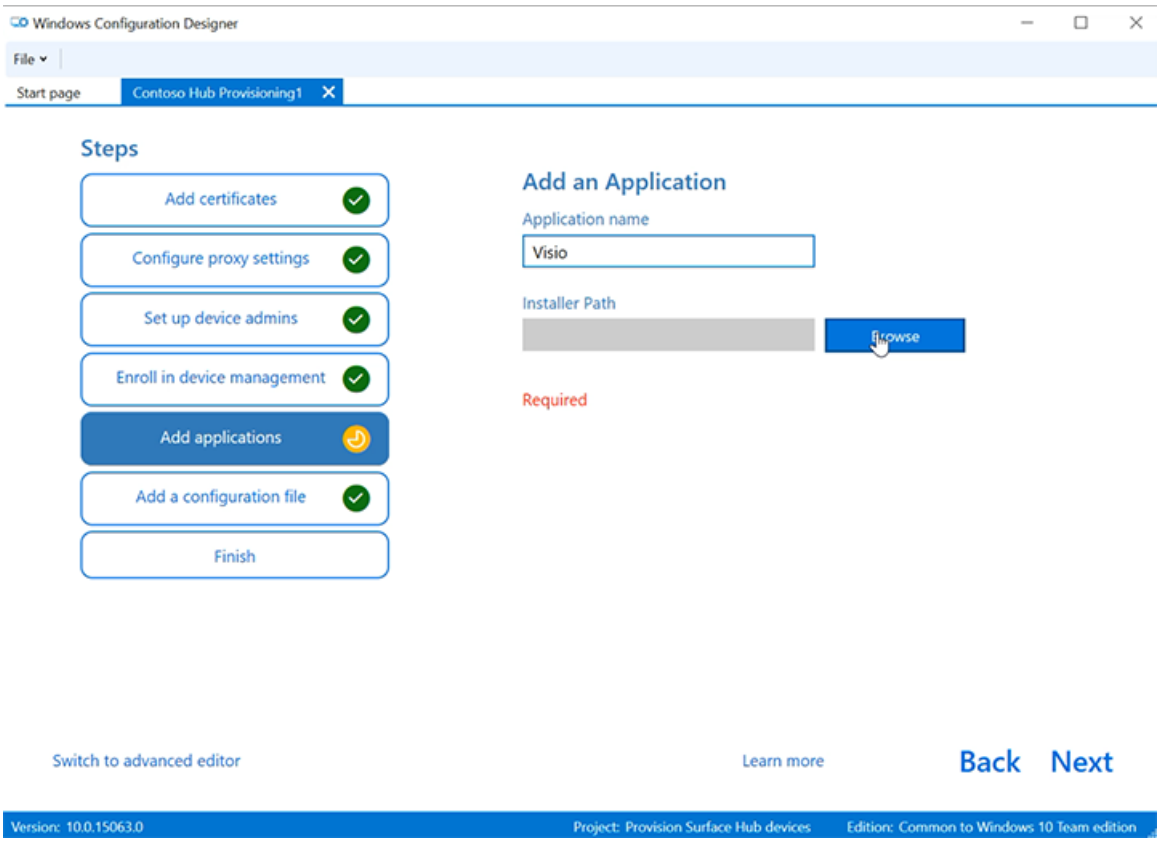


Si usas un proveedor de administración de dispositivos móviles (MDM) de terceros, puedes usar esta sección para inscribir Surface Hub. Para inscribirse en Intune, configure primero la combinación de Azure AD, tal como se describe en la sección anterior, y siga las instrucciones de la siguiente documentación de Intune: Configurar la inscripción automática para dispositivos Windows 10.

1. Alterna **Sí** o **No para** la inscripción en MDM de terceros.
2. Si alterna **Sí**, proporcione una cuenta de servicio y una contraseña o huella digital de certificado que esté autorizada para inscribir el dispositivo y especificar el tipo de autenticación.
3. Si el proveedor mdm lo requiere, escribe las direcciones URL del servicio de detección, el servicio de inscripción y el servicio de directivas.

Para obtener más información, consulta Administrar Surface Hub con un proveedor mdm.

Agregar aplicaciones



Puedes instalar varias aplicaciones para la Plataforma universal de Windows (UWP) en un paquete de aprovisionamiento. Para obtener más información, consulta Aprovisionar equipos con aplicaciones.

> **NOTE**
> Aunque Windows de configuración te permite agregar una aplicación clásica de Win32 a un paquete de aprovisionamiento, Surface Hub solo acepta aplicaciones para UWP. Si incluyes una aplicación Win32 clásica, el aprovisionamiento fallará.

Agregar un archivo de configuración

Además de este paquete de aprovisionamiento, puedes usar un archivo de configuración Surface Hub para facilitar aún más la configuración de los dispositivos. Un archivo de configuración de Surface Hub contiene una lista de cuentas de dispositivo para conectarse a Exchange, Microsoft Teams o Skype Empresarial, así como "nombres descriptivos" para la proyección inalámbrica.

Para crear un archivo Surface Hub de configuración:

1. Abra Microsoft Excel (u otro editor de .csv), cree un archivo .csv denominado *SurfaceHubConfiguration.csv*.
2. Escribe una lista de cuentas de dispositivo y nombres descriptivos en este formato:

```
<DeviceAccountName>,<DeviceAccountPassword>,<FriendlyName>
```

> **NOTE**
> El archivo de configuración no debe contener encabezados de columna. Cuando se incluye en un paquete de aprovisionamiento aplicado a Surface Hub, puedes seleccionar la cuenta y el nombre descriptivo del dispositivo desde el archivo. Para crear el archivo .csv, use un formato de dirección UPN (rainier@contoso.com) o un formato de nombre de inicio de sesión de nivel inferior (contoso\rainier).

rainier@contoso.com,password,Rainier Surface Hub

3. Guarde el archivo en la carpeta del proyecto y cópielo en la clave USB con el paquete de aprovisionamiento.

> **NOTE**
> El archivo de configuración solo se puede aplicar durante la instalación de la primera ejecución.

Paquete de aprovisionamiento de protección de contraseñas

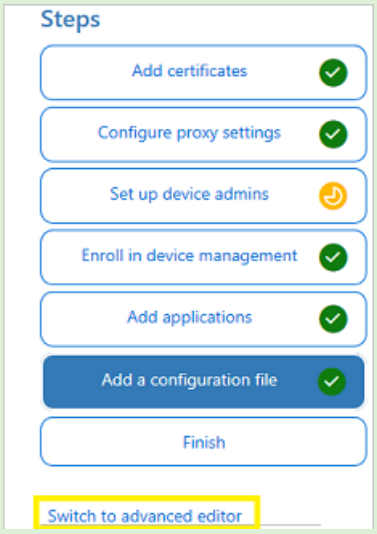
Si eliges usar una contraseña, deberás escribirla cada vez que apliques el paquete de aprovisionamiento a un dispositivo.

Asistente para aprovisionamiento completo

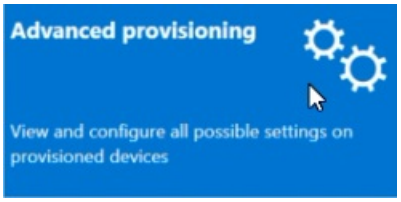
Si solo necesita configurar opciones comunes, seleccione **Finalizar**crear y > **** vaya a la sección Compilar el paquete. O bien, siga configurando la configuración cambiando al aprovisionamiento avanzado.

Usar aprovisionamiento avanzado

> **TIP**
> Usa el asistente para crear un paquete con la configuración común y después usa el editor avanzado para agregar otras configuraciones.

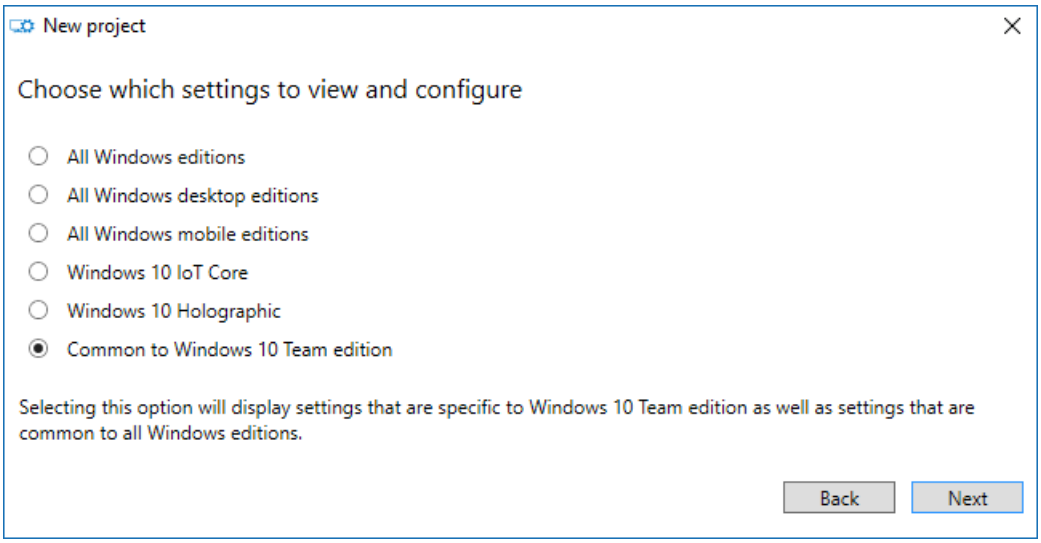


1. Si continúa en la sección anterior, seleccione **Cambiar al editor** avanzado de lo **contrario, abra Windows Diseñador** de configuraciones y seleccione **Aprovisionamiento avanzado**.

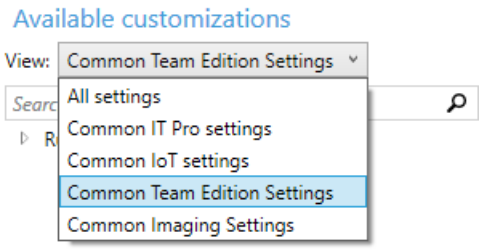


2. Asigne un nombre al proyecto y seleccione **Siguiente**.

3. Seleccione **Común para Windows 10 Team**, seleccione **Siguiente**y, a continuación, seleccione **Finalizar**.



4. En el proyecto, en **Personalizaciones disponibles,** seleccione **Configuración común del equipo**.



Agregar un certificado al paquete

Puedes usar paquetes de aprovisionamiento para instalar certificados que permitirán que el dispositivo se autentique en MicrosoftExchange.

> **NOTE**
> Los paquetes de aprovisionamiento solo pueden instalar certificados en el almacén de dispositivo (máquina local), pero no en el almacén del usuario. Si su organización requiere que los certificados se instalen en el almacén de usuarios, use la aplicación Central **Configuración: Actualizar**& certificados de seguridad > **** > **importar certificado**. Como alternativa, puedes usar directivas **MDM** para implementar certificados en el almacén de dispositivos o en el almacén de usuarios.

> **TIP**
> La **sección ClientCertificates** es para los archivos .pfx con una clave privada; los archivos .cer para las CA raíz deben colocarse en la sección **RootCertificates** y para las CA intermedias en la **sección CACertificates.**

1. En **Windows Configuration Designer** > **Personalizaciones** disponibles, vaya a **Configuración**de tiempo de ejecución > **Certificados** > **ClientCertificates**.
2. Escriba una etiqueta para **CertificateName** y, a continuación, **seleccione Agregar**.
3. Escribe el valor **CertificatePassword**.
4. Para el valor **CertificatePath**, examina y selecciona el certificado.
5. Establece el elemento **ExportCertificate** en **False**.
6. Para **KeyLocation**, selecciona **Software solo**.

Agregar una aplicación para UWP al paquete

Para agregar una aplicación para UWP a un paquete de aprovisionamiento, necesitarás el paquete de la aplicación (archivos .appx o .appxbundle) y los archivos de dependencia. Si adquiriste la aplicación en la

Microsoft Store para Empresas, también necesitarás la licencia de la aplicación *sin codificar*. Consulta Distribuir aplicaciones sin conexión para conocer cómo descargar estos elementos de la Microsoft Store para Empresas.

Para agregar una aplicación para UWP:

1. En el panel **Personalizaciones disponibles**, ve a **Configuración de tiempo de ejecución** > **UniversalAppInstall** > **DeviceContextApp**.
2. Escriba un **PackageFamilyName** para la aplicación y, a continuación, **seleccione Agregar**. Por motivos de coherencia, usa el nombre de familia de paquete de la aplicación. Si adquiriste la aplicación en la Microsoft Store para Empresas, puedes encontrar el nombre de familia de paquete en la licencia de la aplicación. Abra el archivo de licencia con un editor de texto y use el valor entre las etiquetas PFM.
3. Para **ApplicationFile,** seleccione **Examinar** para buscar y seleccionar la aplicación de destino (.appx o .appxbundle).
4. Para **DependencyAppxFiles,** seleccione **Examinar** para buscar y agregar cualquier dependencia para la aplicación. Para Surface Hub, solo necesitas versiones x64 de estas dependencias.

Si adquiriste la aplicación a Microsoft Store para Empresas, deberás agregar la licencia de la aplicación al paquete de aprovisionamiento.

Para agregar una licencia de aplicación:

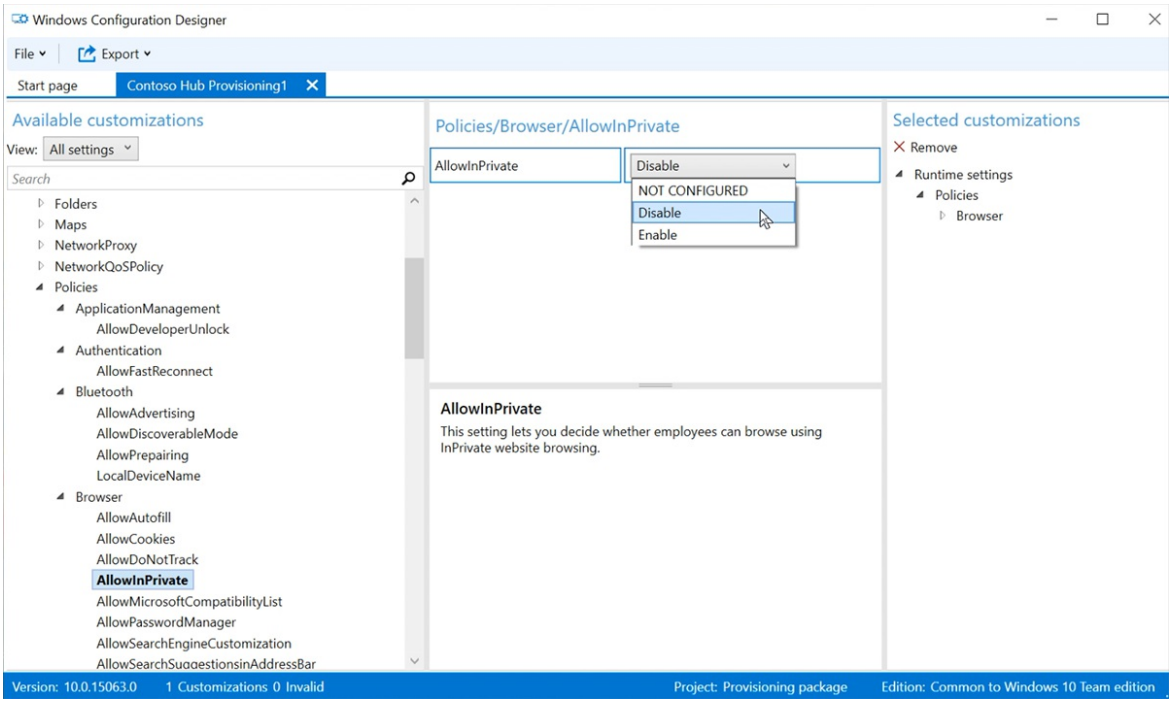
1. Haz una copia de la licencia de la aplicación y cámbiale el nombre para usar una extensión **.ms-windows-store-license**. Por ejemplo, cambie el nombre de "example.xml" a "example.ms-windows-store-license".
2. En Windows Configuration Designer, ve a **Available customizations** > **Runtime settings** > **UniversalAppInstall** > **DeviceContextAppLicense**.
3. Escriba un **LicenseProductId** y, a continuación, **seleccione Agregar**. Por motivos de coherencia, usa el identificador de licencia de aplicación de la licencia de la aplicación. Abre el archivo de licencia con un editor de texto. A continuación, en **la etiqueta License,** use el valor del **atributo LicenseID.**
4. Selecciona el nuevo nodo **LicenseProductId**. Para **LicenseInstall,** seleccione **Examinar** para buscar y seleccionar el archivo de licencia cuyo nombre ha cambiado (example.ms-windows-store-license).

Agregar una directiva al paquete

Surface Hub admite un subconjunto de directivas incluidas en el Proveedor de servicios de configuración de directivas. Algunas de estas directivas se pueden configurar con Windows de configuración.

Para agregar directivas csp:

1. Ve a **Personalizaciones disponibles Configuración de** > **tiempo de ejecución** > **Directivas**.
2. Seleccione el componente que desea administrar y configurar la configuración de directiva según corresponda. Por ejemplo, para impedir que los empleados utilicen la exploración del sitio web de InPrivate en Surface Hub, seleccione **AllowInPrivate** y, a continuación, **seleccione Deshabilitar**.



Agregar valores de configuración de Surface Hub al paquete

Puedes agregar valores de configuración del Proveedor de servicios de configuración de SurfaceHub al paquete de aprovisionamiento.

1. Vaya a **Personalizaciones disponibles** > **Common Team Edition Configuración**.
2. Seleccione el componente que desea administrar y configurar la configuración de directiva según corresponda.
3. Cuando haya terminado de configurar el paquete de aprovisionamiento, seleccione **Guardar** > **archivo**.
4. Lea la advertencia de que los archivos del proyecto pueden contener información confidencial y seleccione **Aceptar**

Crear el paquete

Cuando compilas un paquete de aprovisionamiento, puedes incluir información confidencial en los archivos de proyecto y en el archivo del paquete de aprovisionamiento (.ppkg). Aunque tienes la posibilidad de cifrar el archivo .ppkg, los archivos de proyecto no se cifran. Almacene los archivos del proyecto en una ubicación segura o elimine si ya no es necesario.

1. Abra **Windows paquete de aprovisionamiento de exportación del Diseñador**de > **** > **configuraciones**.
2. Cambiar **propietario a** administrador de **TI.**
3. Establece un valor para **Versión del paquete** y luego selecciona **Siguiente**.

> **TIP**
> Al establecer el propietario en Administrador de TI, se asegura de que la configuración del paquete mantenga las "propiedades de prioridad" adecuadas y permanezca en vigor en Surface Hub si otros paquetes de aprovisionamiento se aplican posteriormente desde otros orígenes.

> **TIP**
> Puede modificar los paquetes existentes y cambiar el número de versión para actualizar los paquetes aplicados anteriormente.

4. Opcional: puede elegir cifrar el paquete y habilitar la firma del paquete:

    a. Seleccione **Cifrar paquete y,** a continuación, escriba una contraseña.
    b. Seleccione **Firmar paquete** > **Examinar** y elija el certificado según corresponda.

    > **IMPORTANT**
    > Se recomienda incluir un certificado de aprovisionamiento de confianza en el paquete de aprovisionamiento. Cuando el paquete se aplica a un dispositivo, el certificado se agrega al almacén del sistema, lo que permite que los paquetes posteriores se apliquen de forma silenciosa.

5. Seleccione **Siguiente** para especificar la ubicación de salida. De forma predeterminada, el Diseñador de configuraciones de Windows usa la carpeta de proyecto como la ubicación de salida. O seleccione **Examinar para** cambiar la ubicación de salida predeterminada. Selecciona **Siguiente**.

6. Seleccione **Compilar** para empezar a compilar el paquete. La información del proyecto se muestra en la página de compilación.

7. Si se produce un error en la compilación, aparecerá un mensaje de error con un vínculo a la carpeta del proyecto. Revise los registros para diagnosticar el error y vuelva a compilar el paquete.

8. Si la compilación se realiza correctamente, se muestra el nombre del paquete de aprovisionamiento, el directorio de salida y el directorio del proyecto. Seleccione **Finalizar** para cerrar el asistente y volver a la página Personalizaciones.

9. Seleccione **la ubicación de** salida para ir a la ubicación del paquete. Copia el archivo .ppkg a una unidad flash USB.

Aplicar un paquete de aprovisionamiento a un dispositivo Surface Hub

Hay dos formas de implementar paquetes de aprovisionamiento en un Surface Hub:

- Ejecute el programa de instalación en primer lugar. Puedes aplicar un paquete de aprovisionamiento para personalizar varias opciones, incluidas la configuración Wi-Fi, la configuración de proxy, los detalles de la cuenta del dispositivo, la unión a Azure AD y la configuración relacionada.
- Configuración aplicación. Después de ejecutar el programa de instalación por primera vez, puedes aplicar un paquete de aprovisionamiento a través Configuración aplicación.

Aplicar un paquete de aprovisionamiento durante la primera ejecución

1. Cuando se activa el Surface Hub por primera vez, el programa de primera ejecución muestra **la página Hi there**. Asegúrate de que las opciones de configuración se hayan configurado correctamente antes de continuar.

2. Inserta la unidad flash USB que contiene el archivo .ppkg en el Surface Hub. Si el paquete está en el directorio raíz de la unidad, el programa de primera ejecución lo reconocerá y preguntará si quieres configurar el dispositivo. Selecciona **Configurar**.

3. La pantalla siguiente te pide que selecciones un origen de aprovisionamiento. Selecciona **Medios extraíbles** y pulsa **Siguiente**.

4. Selecciona el paquete de aprovisionamiento (*.ppkg) que quieras aplicar y pulsa **Siguiente**. Ten en cuenta que solo puedes instalar un paquete durante la primera ejecución.

5. El programa de primera ejecución mostrará un resumen de los cambios que va a aplicar el paquete de aprovisionamiento. Selecciona **Sí, agrégalo**.

6. Si un archivo de configuración se incluye en el directorio raíz de la unidad flash USB, verás **Seleccionar una configuración**. Se mostrará la primera cuenta de dispositivo en el archivo de configuración con un resumen de la información de la cuenta que se aplicará a Surface Hub.

7. En **Seleccionar una configuración,** seleccione el nombre del dispositivo que desea aplicar y, a continuación, **seleccione Siguiente**.

La configuración del paquete de aprovisionamiento se aplicará al dispositivo y se completará la configuración rápida. Una vez reiniciado el dispositivo, puedes quitar la unidad flash USB.

Aplicar un paquete de aprovisionamiento mediante Configuración aplicación

1. Inserta la unidad flash USB que contiene el archivo .ppkg en el Surface Hub.
2. Desde Surface Hub, inicie **Configuración** y escriba las credenciales de administrador cuando se le pida.
3. Navega hasta **Surface Hub** > **Administración de dispositivos**. En **Paquetes de aprovisionamiento, seleccione Agregar o quitar un paquete de aprovisionamiento**Agregar un > **paquete**.
4. Elige el paquete de aprovisionamiento y selecciona **Agregar**. Si se le pide, vuelva a escribir sus credenciales de administrador.
5. Verá un resumen de los cambios que se aplicarán. Selecciona **Sí, agrégalo**.

Obtén más información

- Descargar Windows de configuración
- Crear un paquete de aprovisionamiento para Windows10
- Administrar Surface Hub con un proveedor MDM

Migrar a Windows 10 Pro o Enterprise en Surface Hub 2

12/01/2022 • 15 minutes to read

- Historial de versiones de artículo

Surface Hub 2S viene con Windows 10 Team instalado. Esta edición personalizada de Windows 10 facilita la colaboración en entornos de salas de reuniones. Ahora puede ejecutar en su lugar Windows 10 Pro o Enterprise para usar su Surface Hub 2S como cualquier otro equipo.

> **IMPORTANT**
> Este proceso de migración requiere que siga el procedimiento específico que se describe en este artículo. Antes de continuar, lea Componentes de la solución y Flujo de trabajo de migración e instalación.

> **NOTE**
> Cuando instalas Windows 10 Pro o Enterprise en tu Surface Hub 2S, necesitas una nueva licencia que sea distinta de la licencia Windows 10 Team existente proporcionada con el dispositivo.

Inicia la migración desde Windows 10 Team usando un equipo independiente y la herramienta descargable *Surface UEFI Configurator.* La herramienta crea un paquete que contiene una nueva configuración UEFI que se aplica al Surface Hub 2S.

Surface UEFI Configurator funciona como una interfaz en Surface Enterprise Management Mode (SEMM). Permite la administración centralizada de la configuración de firmware en dispositivos Surface en un entorno corporativo. Para obtener más información, consulta Microsoft Surface Enterprise Management Mode.

Componentes de la solución

- Surface Hub dispositivo 2S que se ejecuta Windows 10 Team
- Dispositivo independiente que se ejecuta Windows 10
- Herramienta Configurador UEFI de Surface para crear el paquete SEMM
- Windows 10 Pro o Enterprise del sistema operativo, versión 1903 o posterior
- Dos unidades USB con 16 GB de almacenamiento, formato FAT32
- Controladores y firmware para Windows 10 Pro y Enterprise en un archivo Surface Hub 2 Microsoft Windows Installer (MSI)
- Conexión a Internet
- Solución de imágenes (opcional)

Resumen de flujo de trabajo de migración e instalación

PASO	ACCIÓN	RESUMEN
1	Compruebe la versión uefi en el Surface Hub 2S.	La versión UEFI debe ser *la 694.2938.768.0* o posterior.

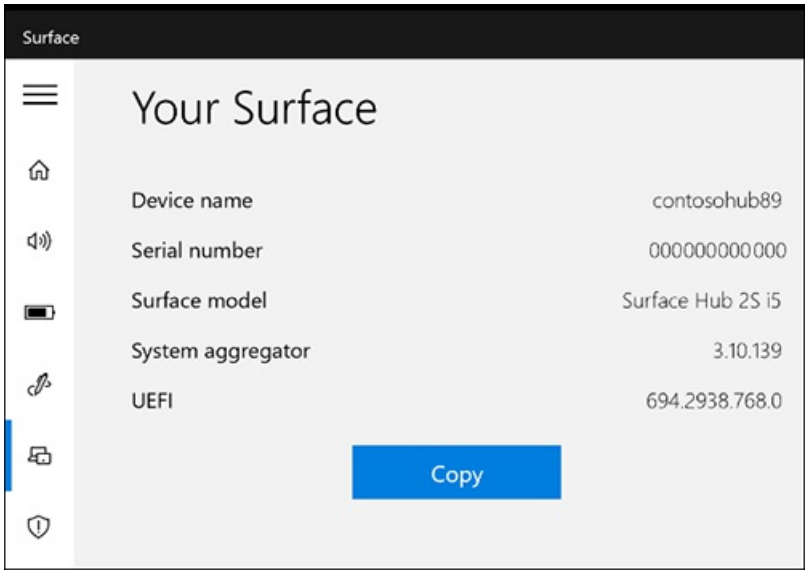
PASO	ACCIÓN	RESUMEN
2	Descarga Surface UEFI Configurator y el Surface Hub 2 controladores y firmware.	En la **página Herramientas de Surface para TI,** selecciona **Descargar**. A continuación, selecciona y descarga el archivo MSI de **UEFI Configurator de Surface**e instálelo en un equipo independiente. Descargue también los controladores y el firmware para Windows 10 Pro y Enterprise sistema operativo en Surface Hub archivo MSI 2. Guarde este paquete para usarlo en el paso 5.
3	Prepare el certificado SEMM.	Prepare el certificado necesario para ejecutar Surface UEFI Configurator o usar el certificado actual.
4	Cree un paquete SEMM.	Inicia Surface UEFI Configurator para crear un paquete SEMM en una unidad USB. Este paquete contendrá los archivos de configuración que necesita aplicar en Surface Hub 2S. Copie estos archivos de paquete SEMM en una carpeta del equipo.
5	Cargue una unidad flash USB con Windows 10 imagen, el paquete SEMM, los controladores y el firmware.	Crea una unidad USB que contenga una Windows 10 imagen. En este ejemplo, la unidad se denomina *BOOTME*. Agregue los controladores y el firmware para el sistema operativo Windows 10 Pro y Enterprise en Surface Hub 2 (del paso 2) y los archivos de paquete SEMM (del paso 4) a la unidad *BOOTME*.
6	Actualice la UEFI en el Surface Hub 2S para habilitar la migración del sistema operativo.	Use la *unidad BOOTME* para arrancar el Surface Hub 2S en el menú UEFI e instalar el paquete SEMM.
7	Instale Windows 10 Pro o Enterprise.	Use la *unidad BOOTME* para instalar Windows 10 Pro o Enterprise versión 1903 o posterior.
8	Instale controladores y firmware para Windows 10 Pro y Enterprise.	Para asegurarse de que el dispositivo tiene todas las actualizaciones y controladores más recientes, instale los controladores y el firmware para Windows 10 Pro y Enterprise sistema operativo en Surface Hub archivo MSI 2.
9	Configura Surface Hub 2S como dispositivo de productividad personal.	Habilita la configuración y las aplicaciones recomendadas para optimizar Surface Hub 2S como dispositivo de productividad personal.

Comprobar la versión UEFI en Surface Hub 2S

Antes de migrar Surface Hub de Windows 10 Team a Windows 10 Desktop, necesita UEFI versión *694.2938.768.0* o posterior.

Para comprobar la versión uefi en el sistema:

1. En la Surface Hub principal de 2S, selecciona **Inicio**y, a continuación, abre la aplicación Surface (**Todas las aplicaciones** > **Surface**).
2. Selecciona **Tu Surface para** mostrar información sobre Surface Hub, incluida la versión actual de UEFI en el dispositivo.
   - Si la versión UEFI es *694.2938.768.0* o posterior, como se muestra en la siguiente imagen, puede crear el paquete SEMM para habilitar la migración del sistema operativo.



   - Si la versión uefi es anterior a la *versión 694.2938.768.0*, use uno de los métodos siguientes para obtener una versión más reciente

Actualizar UEFI a través de Windows Update

1. En el Surface Hub 2S, inicie sesión como **Administrador**.

> **NOTE**
> Si no conoces tu nombre de usuario o contraseña de administrador, tendrás que restablecer el dispositivo. Para obtener más información, vea Reset and recovery for Surface Hub 2S.

2. Ve a **Todas las aplicaciones** > **Configuración** > **Actualización y seguridad**Windows > **actualización**e instala todas las actualizaciones.
3. Reinicia el dispositivo.
4. Comprueba la versión uefi mediante la aplicación Surface. Si la versión UEFI no es *la 694.2938.768.0* o posterior, repita estos pasos o use el siguiente procedimiento para obtener la versión más reciente de UEFI.

Actualizar la UEFI a través de la imagen de recuperación de metal desnudo (BMR)

1. Vaya al sitio de recuperación de Surface y seleccione Surface Hub **2S**.
2. Escriba su número de serie de Concentrador. Se encuentra en la parte posterior del concentrador junto a la conexión de energía.
3. Siga las instrucciones para descargar la imagen en una unidad USB con formato instalando la Windows 10 Team 2020 Update.
4. Después de la actualización, el dispositivo entra en la configuración de la experiencia rápida (OOBE). No es necesario completar la configuración. La versión UEFI ya está actualizada. En su lugar, apaga el dispositivo manteniendo presionado el botón de encendido hasta que se apague la pantalla.

Descargar Surface UEFI Configurator y Surface Hub 2 controladores y firmware

En un equipo independiente, siga estos pasos:

1. En la página Herramientas de Surface para TI, selecciona **Descargar**.
2. Selecciona y descarga el archivo MSI de UEFI Configurator de Surface e instálelo en un equipo independiente. La herramienta Configurador UEFI de Surface no se puede ejecutar en un Surface Hub 2S mientras Windows 10 Team edición está instalada.
3. Descargue el Surface Hub 2 controladores y firmware Windows archivo MSI del instalador. Usará este archivo al instalar el nuevo sistema operativo.

Preparar el certificado SEMM

Si no has usado Surface UEFI Configurator antes, debes preparar un certificado. Este certificado garantiza que, después de inscribir un dispositivo en SEMM, solo puede modificar la configuración de UEFI mediante paquetes creados con el certificado aprobado.

La forma de obtener un certificado depende del tamaño o complejidad de la organización:

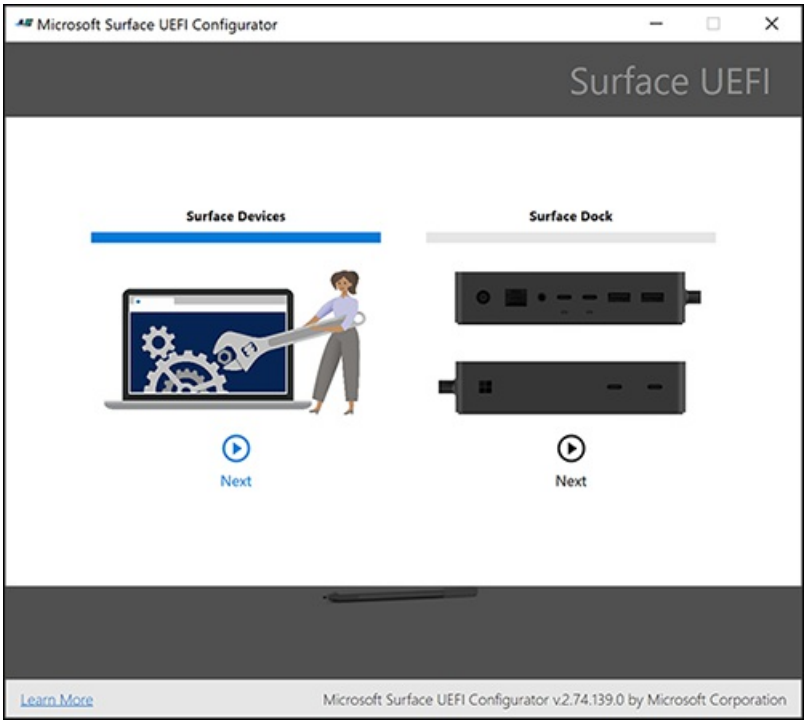
- Enterprise suelen mantener su propia infraestructura para generar certificados de acuerdo con las prácticas de seguridad estándar.
- Las empresas medianas y otras suelen optar por obtener certificados de los proveedores de partners. Esta opción se recomienda para organizaciones que no tienen tanta experiencia en TI o carecen de un equipo de seguridad de TI dedicado.
- Como alternativa, puede generar un certificado autofirmado mediante un script de PowerShell. Para obtener más información, consulta los requisitos del certificado Enterprise modo de administración de Surface. O puede usar PowerShell para crear su propio certificado. Para obtener más información, consulte la documentación del certificado autofirmado.

El paquete SEMM que crea Surface UEFI Configurator debe protegerse con un certificado. El certificado comprueba la firma de los archivos de configuración antes de poder aplicar la configuración de UEFI. Para obtener más información, consulte la documentación de SEMM.

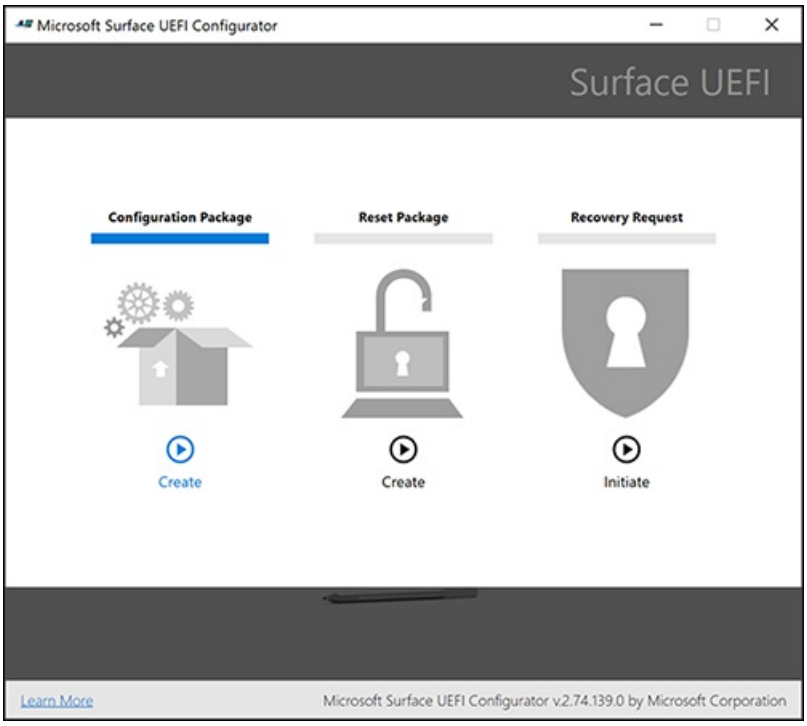
Crear un paquete SEMM

1. En un equipo independiente, instala la herramienta Configurador de UEFI de Surface que descargaste anteriormente.
2. Abra El Configurador UEFI de Surface y, a continuación, **seleccione Inicio**.

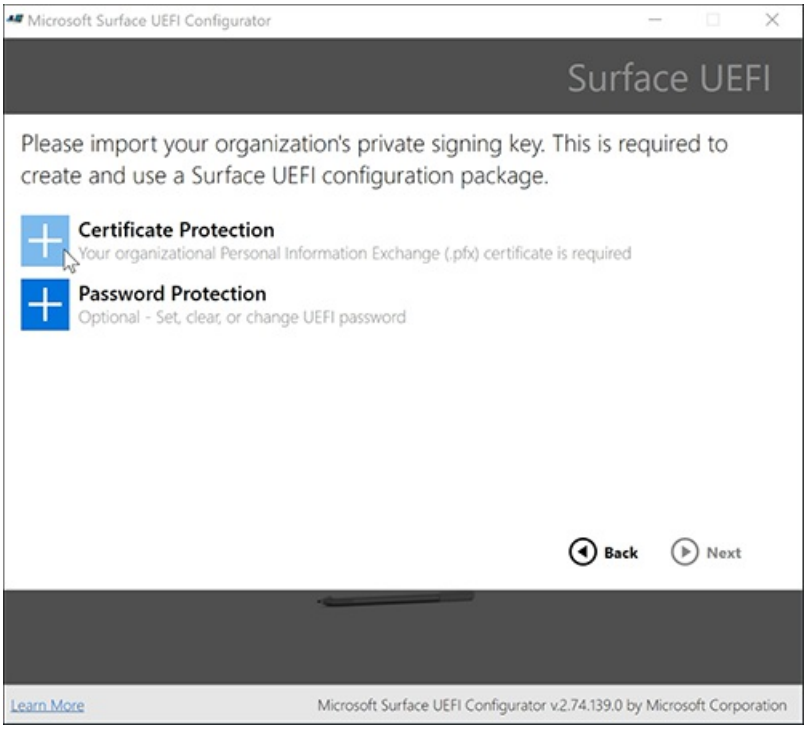
3. Selecciona **Dispositivos Surface**y, a continuación, **selecciona Siguiente**.



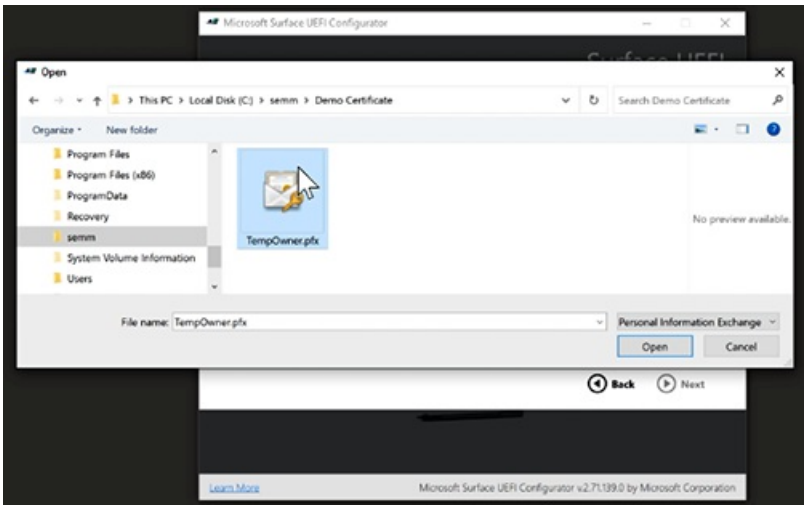
4. Seleccione **Paquete de configuración**.



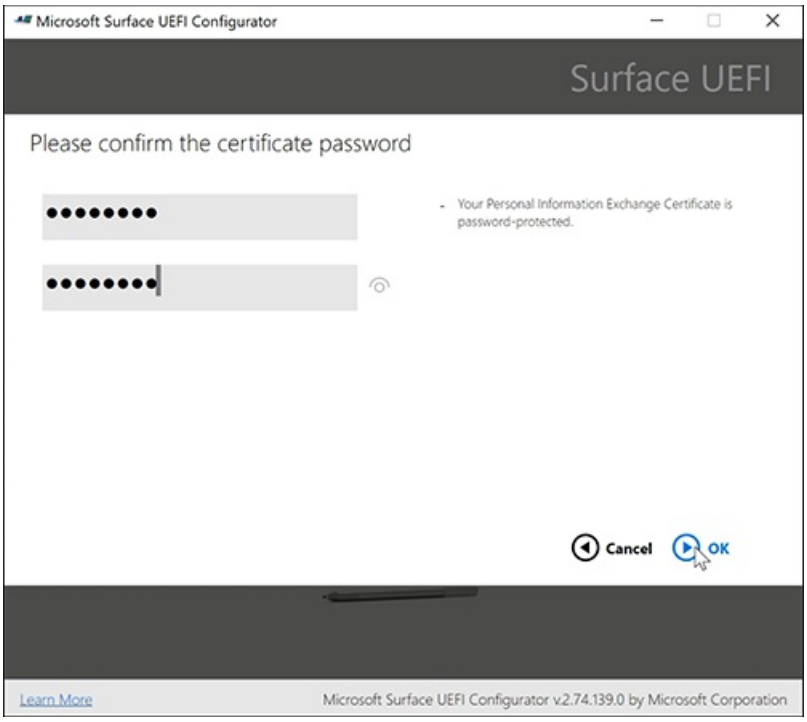
5. Seleccione **Protección de certificados**.



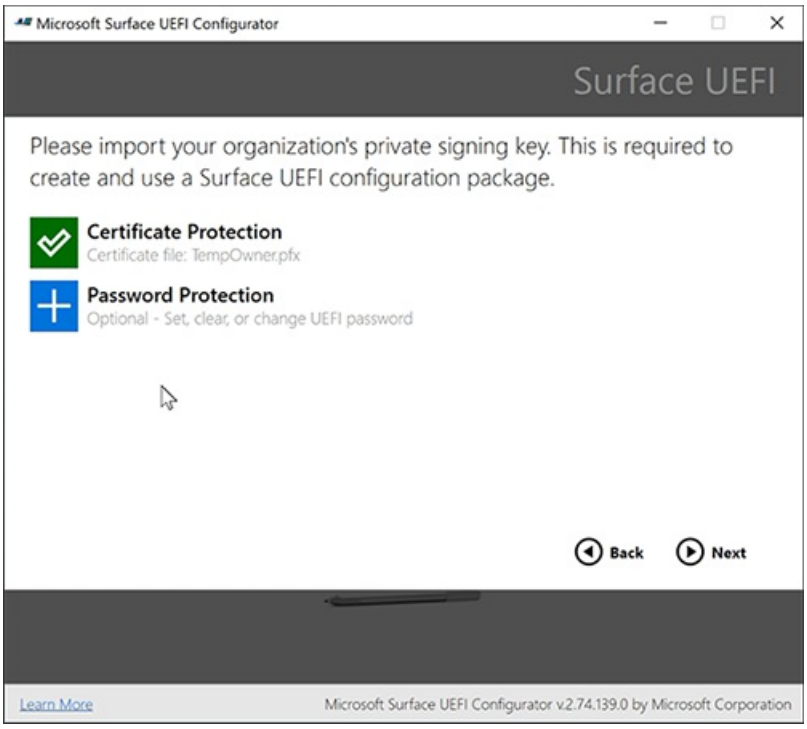
Se le pedirá que agregue el archivo .pfx del certificado.



6. Escriba la contraseña del certificado y, a continuación, **seleccione Aceptar**.

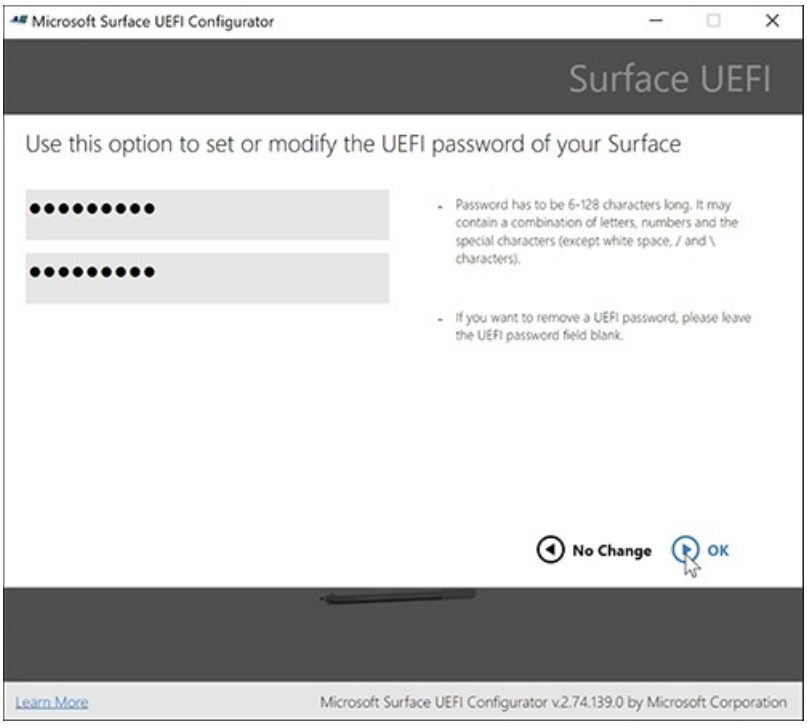


7. Selecciona **Protección con contraseña** para agregar una contraseña a la UEFI de Surface. Necesitarás esta contraseña siempre que arranques en la UEFI. *Le recomendamos encarecidamente que establezca una contraseña UEFI que usará en Surface Hub 2S.*

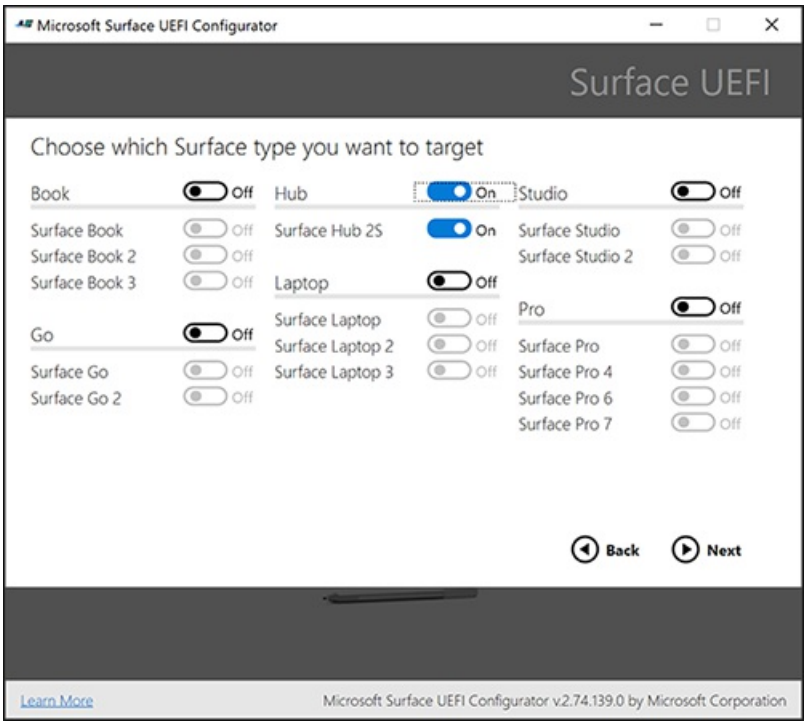


8. Establezca una contraseña uefi y, a continuación, seleccione **Aceptar**.

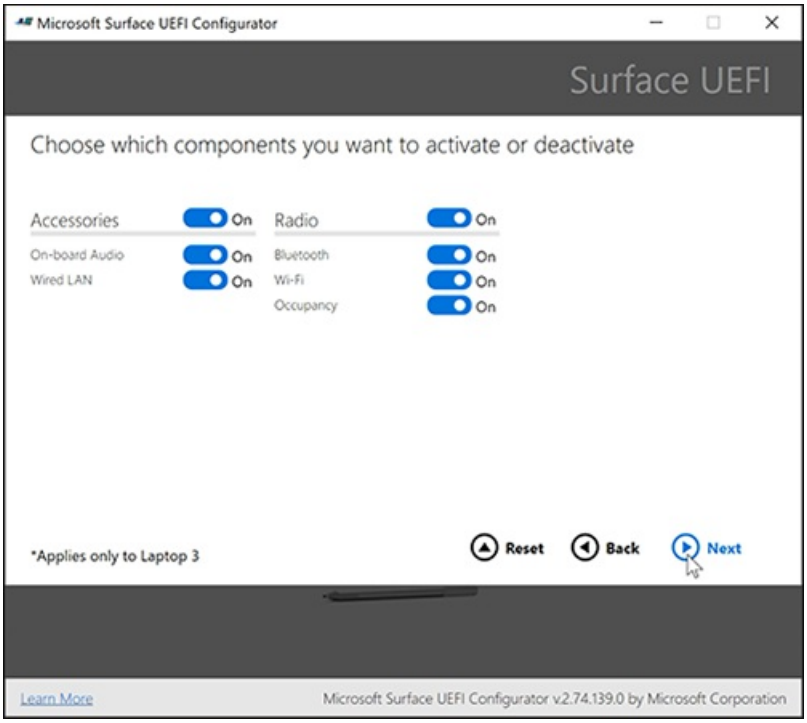
> **IMPORTANT**
>
> Guarde la contraseña en una ubicación segura a la que puedan acceder los administradores de TI que administran Surface Hub. *Si se pierde esta contraseña, no se puede recuperar.*



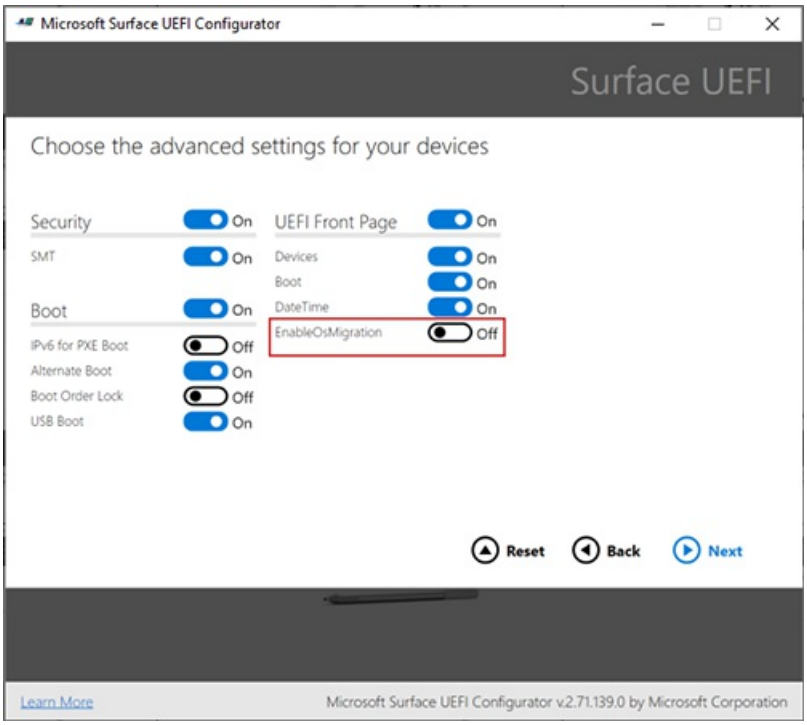
9. Seleccione **Surface Hub 2S**y, a continuación, **seleccione Siguiente**.

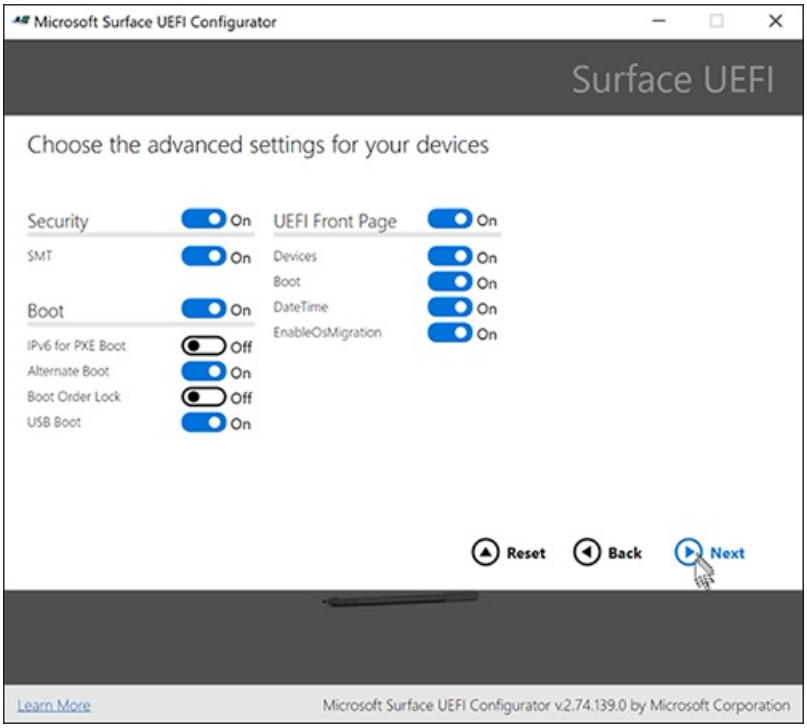


10. Vuelva **a seleccionar** Siguiente.



11. Para permitir la instalación de Windows 10 Pro o Enterprise, active **EnableOsMigration**y, a continuación, seleccione **Siguiente**.





Administrar la inscripción de SEMM

Inscribir un dispositivo en SEMM afecta a la forma en que puedes administrarlo. Por ejemplo, después de aplicar un paquete SEMM, todas las configuraciones de UEFI no están disponibles (bloqueadas) en el menú UEFI del dispositivo. Los valores predeterminados de otras configuraciones, como **IPv6 para arranque PXE**, tampoco están disponibles.

Para cambiar la configuración de UEFI después de finalizar la migración, aplique otro paquete SEMM o desenrolle el dispositivo desde SEMM. Si aplica otro paquete SEMM para cambiar la configuración de UEFI, debe usar el certificado original al compilar el nuevo paquete SEMM. Use la herramienta Configurador UEFI y deje **EnableOSMigration** desactivado *(no como* en los pasos de migración originales).

Si trabaja con partners

Si su empresa subcontrata la migración de Surface Hub 2 a Windows 10 Pro o Enterprise, es posible que desee que el partner le transfiera el certificado SEMM, el paquete SEMM y la contraseña UEFI. O bien, después de migrar el concentrador, puede desenrollar inmediatamente desde SEMM. Este paso permite la administración

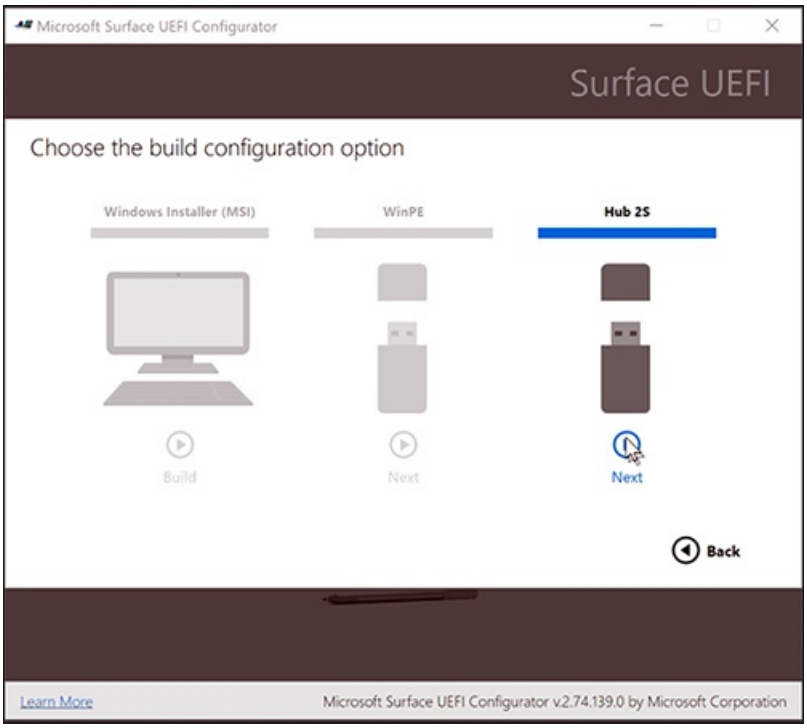
local de UEFI y la transferencia del dispositivo a otra parte. Sin embargo, se recomienda encarecidamente que use una contraseña UEFI, que se puede configurar después de la migración. Para obtener más información, consulta Administrar la configuración de UEFI de Surface.

Para revertir a Windows 10 Team

Si eliges restaurar el dispositivo a Windows 10 Team después de la migración, como se describe más adelante en este artículo,te recomendamos que primero desenrolles Hub de SEMM. Para obtener más información, consulta Unenroll Surface devices from SEMM.

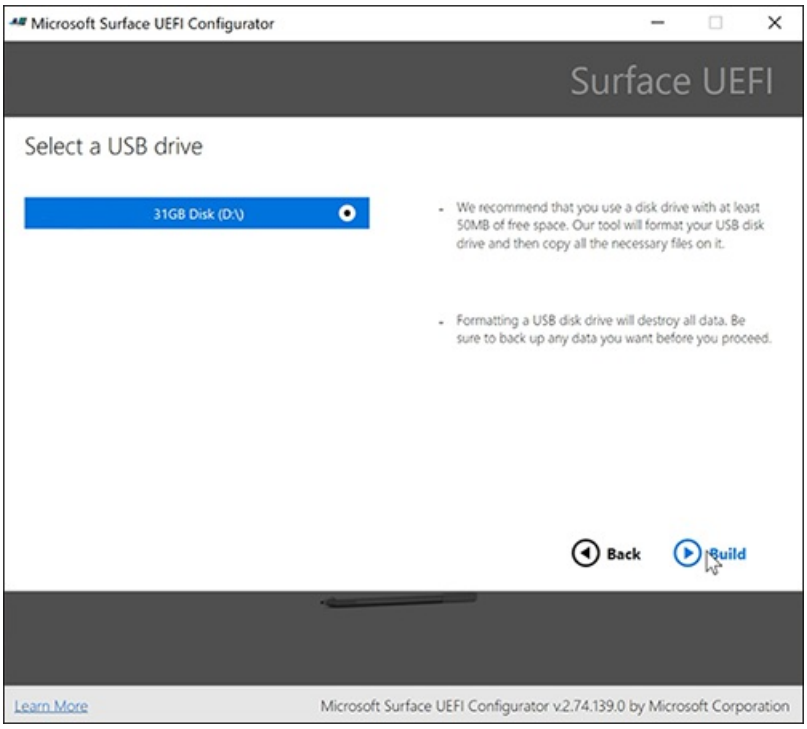
Guardar el paquete SEMM en una unidad USB

1. Conectar una unidad USB al equipo.
2. Elija **Concentrador 2S**y, a continuación, **seleccione Siguiente**.

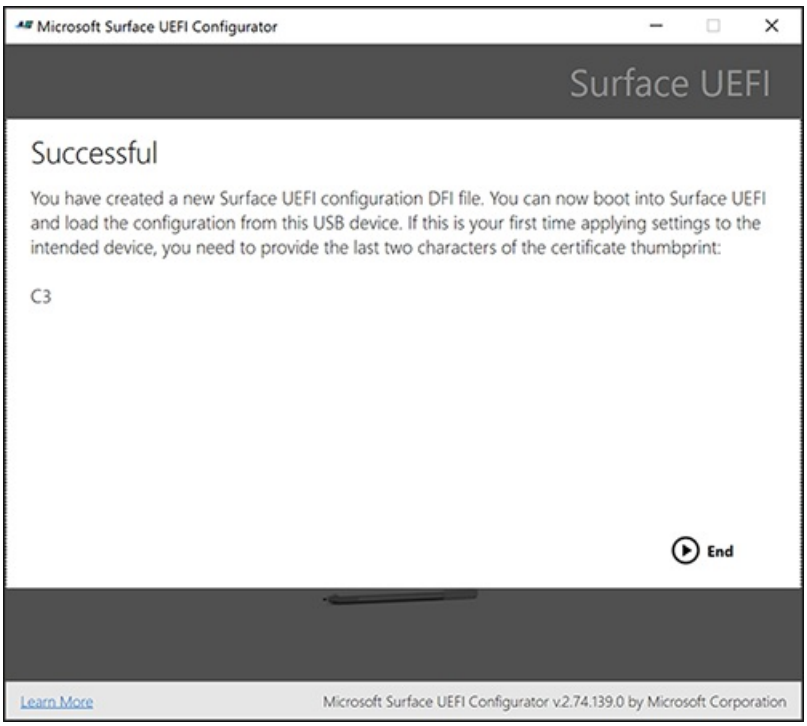


> **WARNING**
> Todos los datos existentes en la unidad USB se borrarán cuando se haya creado el paquete SEMM. Antes de crear el paquete SEMM, quite los archivos que necesite de la unidad USB.

3. Seleccione **Generar**.



4. Captura una captura de pantalla de esta página y, a continuación, selecciona **Finalizar**. El paquete SEMM ya está listo. Contiene el paquete SEMM *DfciUpdate.dfi* y un archivo de texto que incluye la huella digital de *SEMM*, que son los dos últimos caracteres de la huella digital del certificado.



5. Guarde los dos últimos caracteres de la huella digital del certificado. Necesitarás estos caracteres para activar SEMM cuando apliques el paquete en Surface Hub 2S.

Cargar una unidad flash USB con una imagen Windows 10, un paquete SEMM y Surface Hub 2 controladores y firmware

Puede instalar una imagen Windows 10 Pro o Enterprise (versión *1903* o posterior) mediante una de las siguientes opciones:

- La solución de imágenes actual.
- Acelerador de implementación de Surface. Use esta herramienta para crear una imagen Windows 10 arranque. La imagen puede incluir todas las actualizaciones Windows 10, Microsoft Office, otras

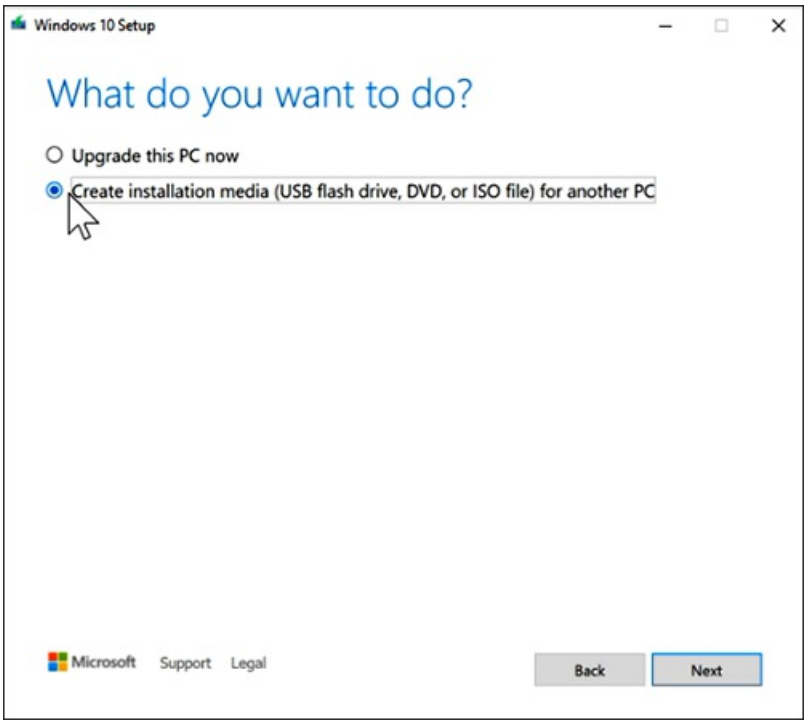
aplicaciones y los controladores y firmware necesarios.

- Una unidad flash USB que contiene una Windows 10 Pro o Enterprise imagen. Esta opción no tendrá Wi-Fi disponible hasta después de la configuración de la experiencia de salida (OOBE). Una vez completada la instalación, instale el Surface Hub 2 controladores y firmware para Windows 10 Pro y Enterprise en el dispositivo.

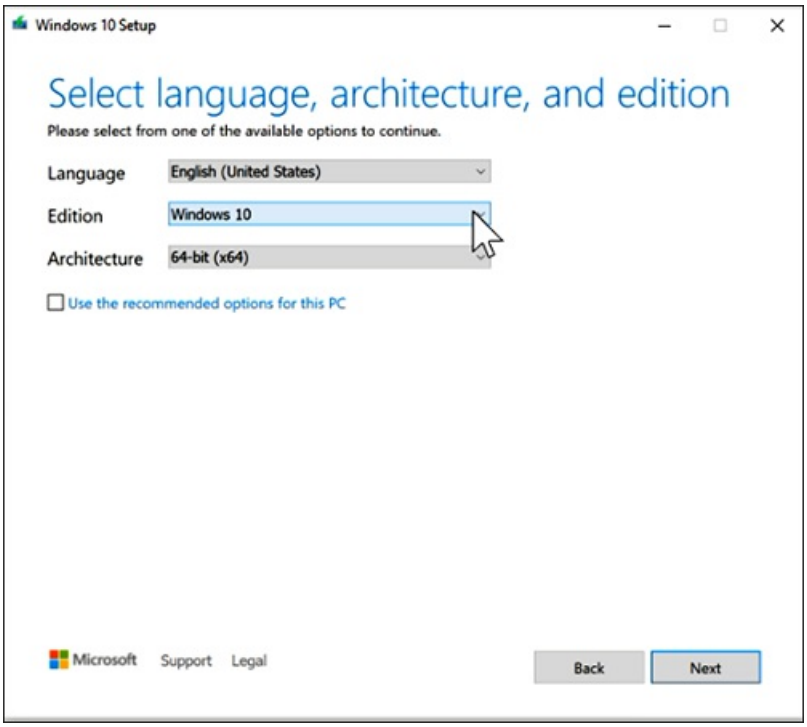
En los pasos siguientes se muestra cómo crear una unidad flash USB a partir de medios de instalación y, a continuación, agregar los archivos de paquete SEMM y los controladores y firmware para el sistema operativo Windows 10 Pro y Enterprise en un archivo MSI Surface Hub 2. Si usa otro método de implementación, vaya a la sección Actualizar UEFI en Surface Hub 2S para habilitar la migración del sistema operativo de este artículo.

> **NOTE**
> Después de finalizar la instalación, necesitará una licencia válida para Windows 10 Pro o Windows 10 Enterprise que sea independiente de la licencia de Windows 10 Team existente.

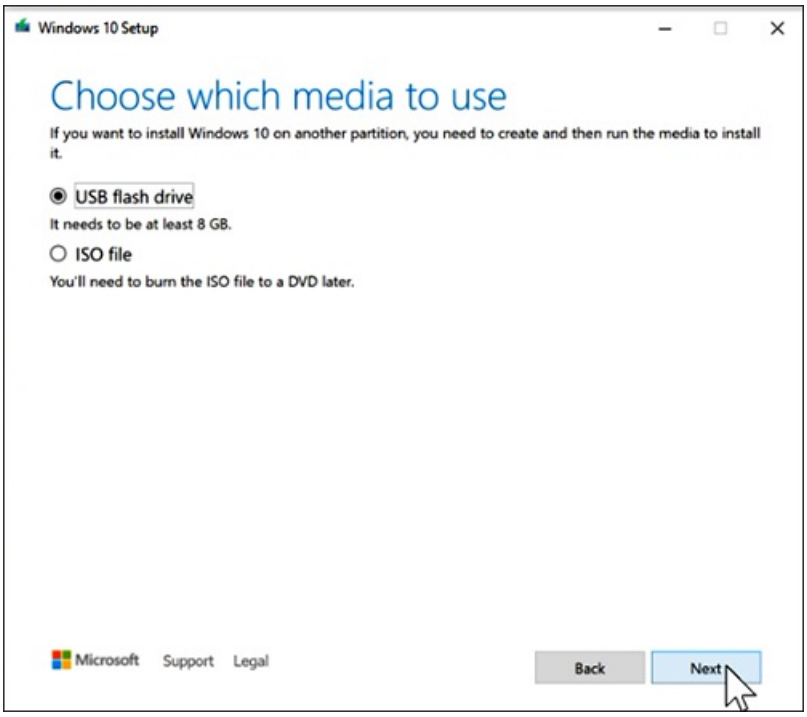
1. Para crear una instalación Windows 10 Pro, siga las instrucciones para descargar la herramienta de creación de medios en Descargar Windows 10. Para descargar Windows 10 Enterprise, vaya al Centro de servicios de licencias por volumen de Microsoft.
2. Inserte una nueva unidad de almacenamiento USB.
3. Abra la herramienta de creación de medios, **seleccione Crear medios de instalación**y, a continuación, seleccione **Siguiente**.



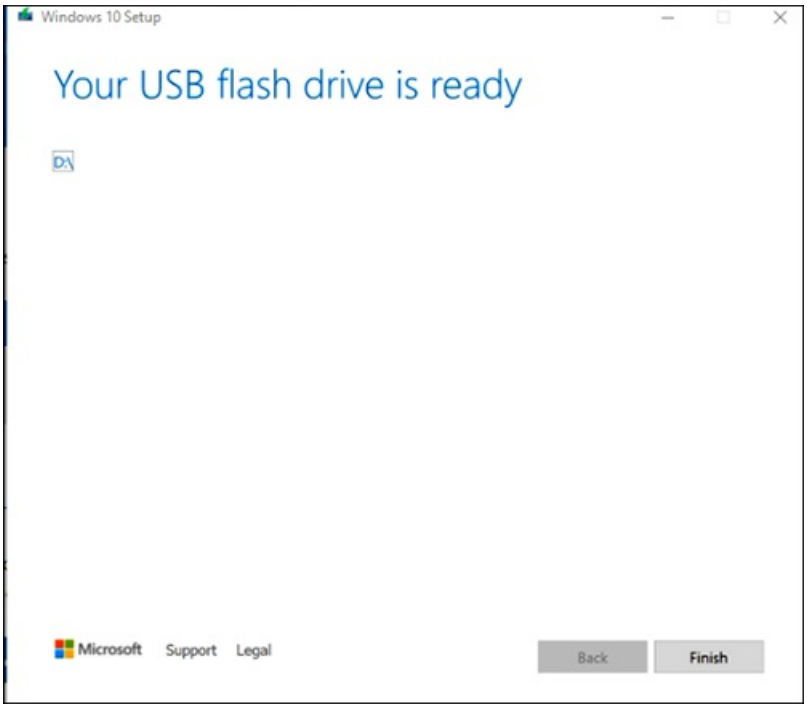
4. Seleccione un idioma y, a **continuación, seleccione Windows 10** y **64 bits (x64).** A continuación, **seleccione Siguiente**.



5. Seleccione **Unidad flash USB**y, a continuación, seleccione **Siguiente**.



6. Cuando finalice la descarga, seleccione **Finalizar**.



7. Copie los archivos del paquete SEMM, los controladores y el firmware del sistema operativo Windows 10 Pro y Enterprise en Surface Hub 2 (el archivo MSI) en la raíz de la unidad flash USB (*BOOTME*) que contiene la imagen Windows 10. La unidad USB BOOTME contendrá:

   - La Windows 10 de arranque.
   - Los archivos de paquete SEMM, copiados en la raíz de la unidad USB:
     - *DfciUpdate.dfi*.
     - Un archivo de texto que incluye la huella digital de SEMM. (En este ejemplo, el archivo *SurfaceUEFI_2020Aug25_1058.txt*.) La marca de fecha y hora generada automáticamente corresponde a la fecha en que creaste el archivo mediante Surface UEFI Configurator.
   - Controladores y firmware para Windows 10 Pro y Enterprise sistema operativo en Surface Hub 2 (SurfaceHub2S_Win10_18362_20.082.25682.0.msi). Copie este archivo en la raíz de la unidad USB.

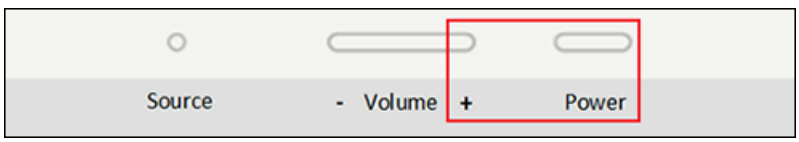
Actualizar UEFI en Surface Hub 2S para habilitar la migración del sistema operativo

1. Inserte la unidad BOOTME en el puerto USB-A del Surface Hub 2S. Para obtener una lista de su contenido necesario, consulte la sección anterior.

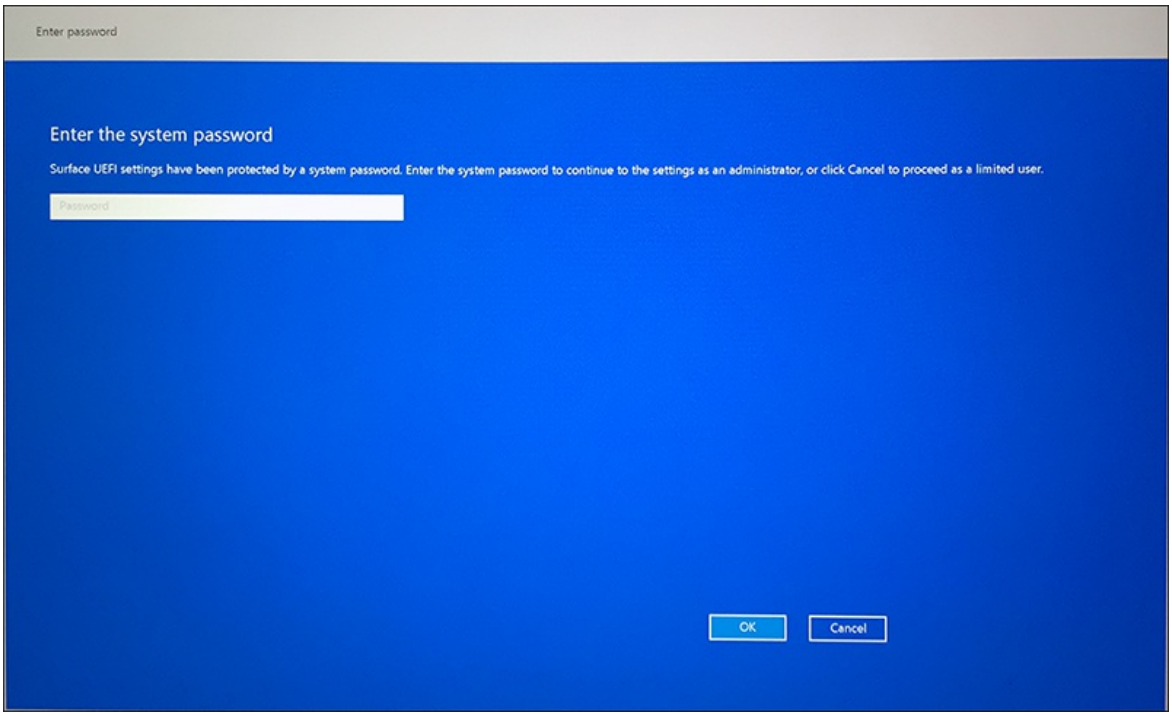
2. Para arrancar en UEFI:

   a. Desactiva (apaga) el Surface Hub 2S.

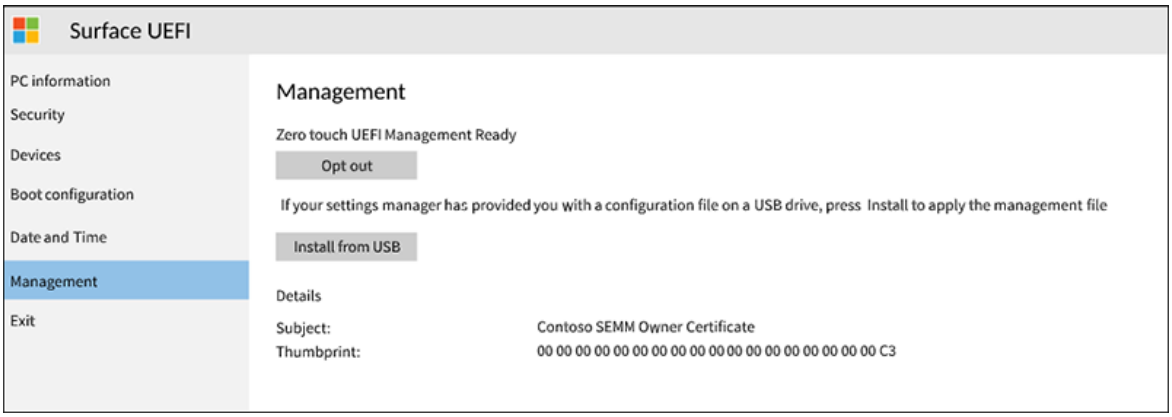
   b. Mantenga presionado **El volumen +** y, a continuación, presione y suelte el botón de encendido. Mantenga presionado **El volumen +** hasta que aparezca el menú UEFI.



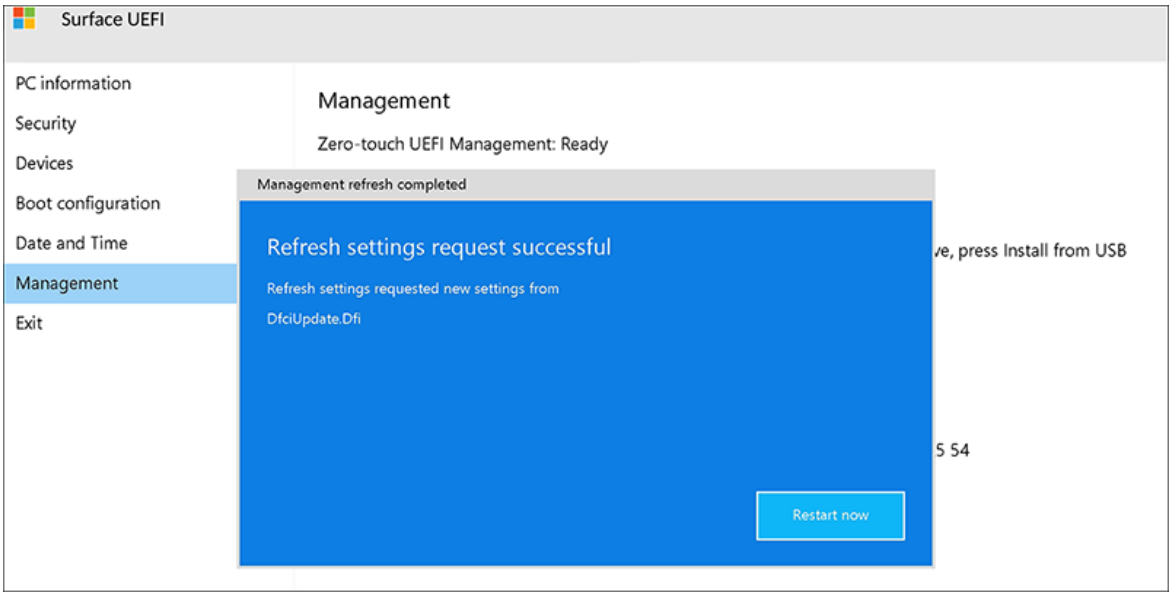
3. Cuando se reinicie el dispositivo, escriba la contraseña UEFI que creó anteriormente, si procede (recomendado).



4. En el menú UEFI, seleccione **Administración**. A **continuación, seleccione Instalar desde USB**.



5. Seleccione **Reiniciar ahora**, como se muestra en la siguiente imagen. El dispositivo se reiniciará. Se mostrará un logotipo blanco de Microsoft en el centro de la ventana y, a continuación, se apagará.



6. Presione y suelte el botón de encendido. En el cuadro de diálogo rojo que aparece, elige activar Surface Enterprise Modo de administración.

7. Escriba la huella digital del certificado de dos caracteres y la contraseña de configuración de UEFI. A continuación, **seleccione Aceptar**.

> **NOTE**
>
> Después de activar SEMM en el dispositivo, se aplica la nueva configuración de UEFI **EnableOSMigration**. Ya no puede acceder a Windows 10 Team. En su lugar, debe continuar con el siguiente paso e instalar Windows 10 Pro o Windows 10 Enterprise.

El dispositivo se reinicia. Muestra el logotipo blanco en el centro de la pantalla y, a continuación, se apaga de nuevo.

Instalar Windows 10 Pro o Enterprise

1. Si la unidad Windows 10 Pro o Enterprise de arranque no está ya en el puerto USB-A Surface Hub 2, insértela ahora. A continuación, presione y suelte el botón de encendido.

   Cuando se inicie el dispositivo, verás el logotipo blanco en el centro de la pantalla. A continuación, aparece un círculo giratorio debajo del logotipo blanco.

2. Si el dispositivo Surface no arranca automáticamente en la unidad USB, apaga el dispositivo (desconecta el cable de alimentación y vuelve a conectarlo). Después de volver a conectar el cable de alimentación, el dispositivo debe arrancar después de unos segundos. A continuación, verás el logotipo blanco en el medio de la pantalla.

   Si el dispositivo no se enciende, presione y suelte el botón de encendido. Inmediatamente después de ver el logotipo en el centro de la pantalla, presione y mantenga presionado el botón Bajar volumen hasta que vea el círculo giratorio debajo del logotipo blanco.

3. Cuando se inicie la configuración de la experiencia lista para usar (OOBE), siga las instrucciones para instalar Windows 10 Pro o Enterprise (versión 1903 o posterior).

Instalar Surface Hub 2 controladores y firmware

Para asegurarse de que el Surface Hub 2 está actualizado, instale controladores y firmware para Windows 10 Pro y Enterprise. A continuación, reinicie el dispositivo. Mantén la Surface activada durante una hora y, a continuación, vuelve a reiniciarla. No se le pedirá el segundo reinicio. Esta pausa y reinicio adicional garantiza que el firmware se haya actualizado por completo.

Configurar las opciones recomendadas

Para configurar Surface Hub 2S como dispositivo de productividad personal, consulta Configurar Windows 10 Pro o Enterprise en Surface Hub 2.

> **NOTE**
> Si no puedes migrar correctamente el dispositivo a Windows 10 Pro o Enterprise para Surface Hub 2 siguiendo los pasos descritos en este artículo, ponte en contacto Surface Hub Soportetécnico .

Para revertir a Windows 10 Team

Si quieres restaurar el dispositivo a Windows 10 Team, consulta Restablecer y recuperar para Surface Hub 2S.

> **NOTE**
> Antes de volver a Windows 10 Team, le recomendamos que primero desenrolle el Surface Hub de SEMM. Para obtener más información, consulta Unenroll Surface devices from SEMM.

Historial de versiones

En la tabla siguiente se resumen los cambios realizados en este artículo.

VERSIÓN	FECHA	DESCRIPCIÓN
v. 1.4	14 de diciembre de 2020	Proporciona más información acerca de la instalación del archivo MSI para "Controladores y firmware para el sistema operativo Windows 10 Pro y Enterprise en Surface Hub 2", lo que aconseja que sea necesario un segundo reinicio en función del estado del sistema.
v. 1.3	3 de diciembre de 2020	Se actualizó con instrucciones sobre cómo administrar la inscripción de SEMM.
v. 1.2	29 de septiembre de 2020	Actualizaciones misceláneas que abordan los comentarios de facilidad de uso.
v. 1.1	15 de septiembre de 2020	Se ha colocado una nota adicional en la introducción que aclara los requisitos de licencias para instalar un nuevo sistema operativo.
v. 1.0	1 de septiembre de 2020	Nuevo artículo.

Configurar Windows 10 Pro o Enterprise en Surface Hub 2

12/01/2022 • 18 minutes to read

Después de completar el proceso de instalación de la migración a Windows 10 Pro o Enterprise, puede realizar los siguientes pasos para configurar aplicaciones y opciones en su Surface Hub 2. Estos pasos se recomiendan para garantizar la mejor experiencia al usar este equipo táctil y de lápiz de pantalla grande personalizado.

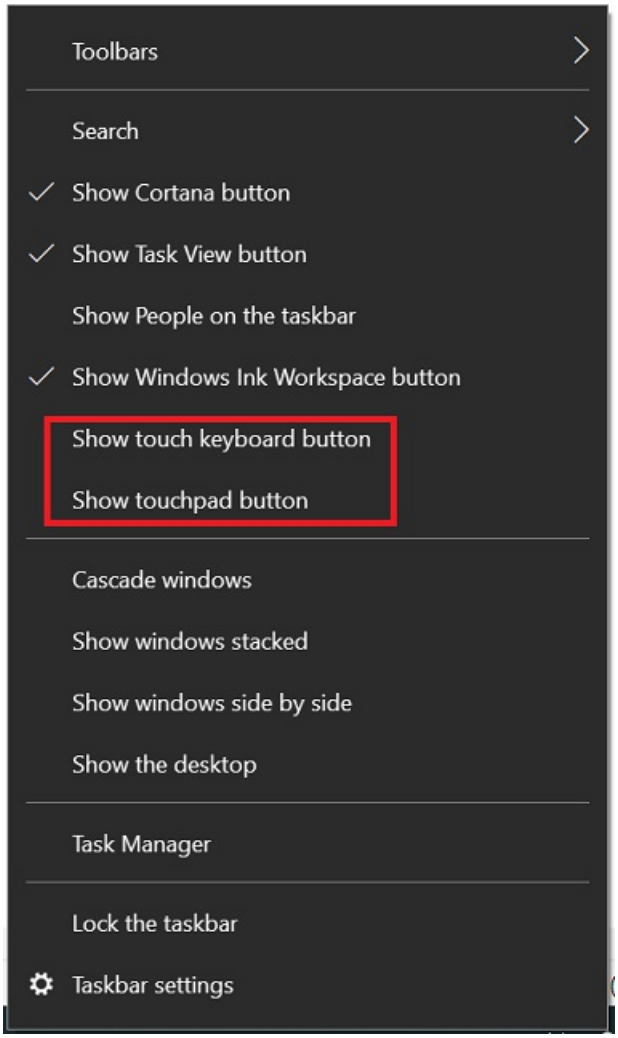
Al realizar estos pasos, puede resultar útil usar un teclado y un mouse con cable o inalámbrico.

Configurar la configuración del sistema

1. Inicie sesión con una cuenta que tenga privilegios de administrador local en el dispositivo.
    - En los dispositivos unidos a Azure AD, el usuario que realiza la unión a Azure AD se agrega automáticamente al grupo de administradores local. Los administradores globales de Azure AD y los dispositivos de Azure AD también son administradores locales.
    - Puede escribir **administradores de grupos locales netos** en un símbolo del sistema para enumerar las cuentas que tienen derechos de administrador local.
2. Cambie el nombre del dispositivo con un nombre descriptivo, por ejemplo: **username-SHub-Desktop**.
3. Selecciona **Iniciar** > **Configuración** > **Cuentas** > **Sincronizar la configuración y** desactivar la configuración de **sincronización.**
    - La configuración que se usa aquí está diseñada para habilitar la mejor experiencia táctil de pantalla grande y, por lo tanto, es posible que no quiera sincronizar otros dispositivos.
4. Reinicia el dispositivo.

Habilitar el teclado táctil y el panel táctil

1. Selecciona **Inicio** > **Configuración** > **Dispositivos de**escritura y activa Mostrar el teclado táctil cuando > **** **no** esté en modo tableta y no haya ningún teclado conectado.
2. Pulse y mantenga presionado o haga clic con el botón secundario en la barra de tareas y, a continuación, seleccione **Mostrar botón del teclado táctil** y Mostrar botón del panel **táctil.**
    - El teclado táctil es útil para la entrada directa del usuario y el panel táctil virtual ayuda con selecciones precisas, sugerencias de pantalla activa o como alternativa para pulsar y mantener pulsado el botón secundario.
    - Consulta el ejemplo siguiente:



3. Configure el teclado táctil en QWERTY y flotante.

   a. Seleccione el **icono Teclado** de la barra de tareas para mostrar el teclado táctil.

   b. En el teclado táctil, selecciona el icono del teclado en la esquina superior izquierda para abrir la configuración del teclado.

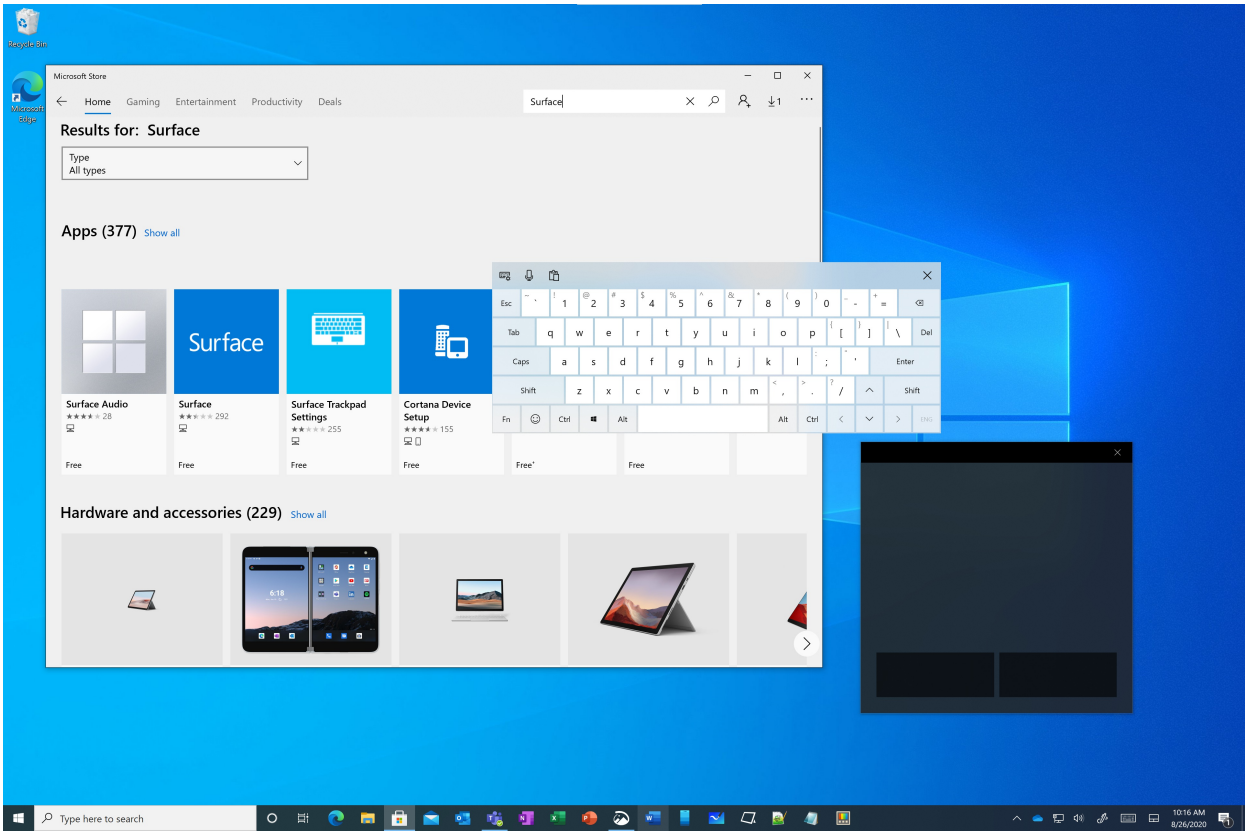
   c. Seleccione el tipo de teclado junto al último de la fila superior para habilitar QWERTY y la última opción de la segunda fila para habilitar flotante, lo que resulta muy útil en esta pantalla grande. Vea los ejemplos siguientes:

4. Configure las opciones de teclado suave.

   a. Seleccione el **Configuración** en el teclado táctil o busque y abra **La configuración de escritura.**

b. Habilita todas las opciones en Ortografía, Escritura y teclado táctil.

En el ejemplo siguiente se muestra el trackpad, que resulta útil para navegar y seleccionar opciones. El teclado en pantalla se usa para buscar en el Microsoft Store:



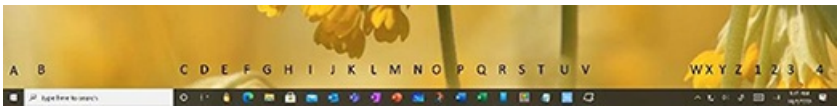
Configurar Bluetooth teclado y mouse (opcional)

Conectar un teclado y un mouse si usas el dispositivo como dispositivo Windows principal, o lo usas a menudo para escribir o trabajar con precisión.

Si el Surface Hub está cerca de un equipo, puedes usar Mouse sin bordes para moverse sin problemas entre el Surface Hub y el equipo. Para obtener más información, consulta Descarga de Microsoft desde El garage: Mouse sin bordes.

Ejemplo de diseño de la barra de tareas

Después de completar los pasos siguientes para configurar o configurar su Surface Hub 2 para Windows 10 Professional o Enterprise, le recomendamos que use anclar las aplicaciones más usadas a la barra de tareas para un inicio rápido de un solo toque de cada aplicación. A continuación se muestra un ejemplo de cómo podría ser la barra de tareas:



Actualizar aplicaciones instaladas

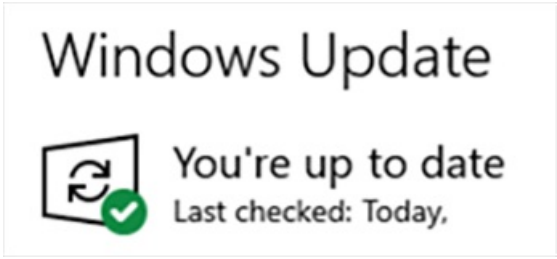
Para actualizar todas las aplicaciones de la Tienda instaladas:

1. Abre Microsoft Store aplicación y selecciona **los** puntos suspensivos Ver más en la esquina superior derecha.
2. Selecciona **Descargas y actualizaciones.**
3. Seleccionar **Obtener actualizaciones**

Buscar e instalar todas las Windows actualizaciones

Después de migrar a Windows 10 Professional o Windows 10 Enterprise, puede haber actualizaciones de mantenimiento y características disponibles para su instalación.

- Vaya a **Configuración** > **Actualizar & seguridad** > y, a continuación, seleccione **Buscar actualizaciones**.
- Si hay actualizaciones, instáleslas, reinicie y repita el proceso hasta que vea la siguiente notificación:

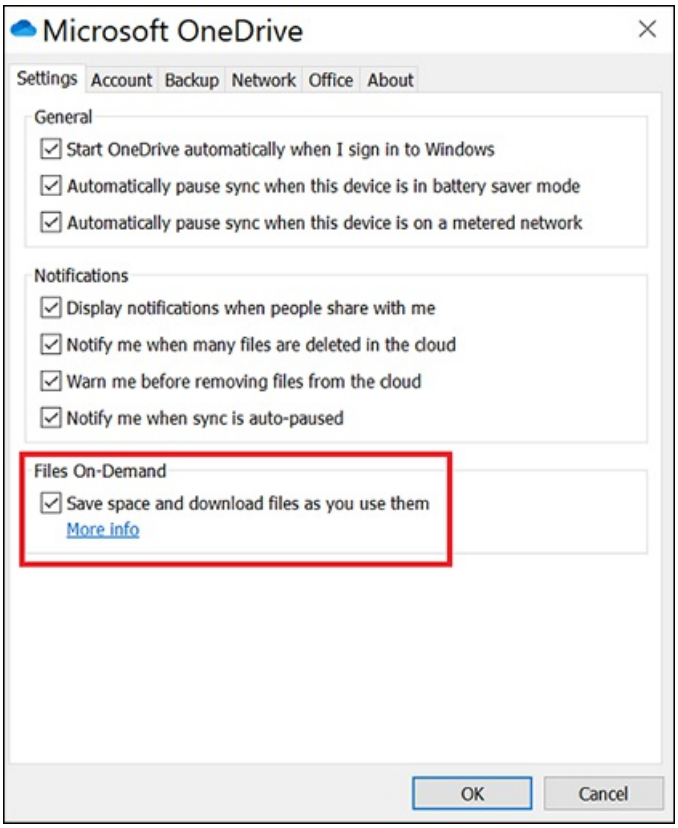


OneDrive para la Empresa

Usa OneDrive para la Empresa para compartir fácilmente herramientas, registros y otros archivos entre todos los dispositivos de trabajo.

- OneDrive permite compartir los archivos de trabajo entre los portátiles, Surface Hub escritorio y los dispositivos móviles administrados por Intune. Los archivos se pueden editar en cualquier dispositivo y todos los dispositivos conectados a la red se actualizarán con los cambios.
- Teniendo en cuenta el tamaño del SSD de Surface Hub (128 GB), si configuras OneDrive en el dispositivo de escritorio de Surface Hub, asegúrate de que la configuración predeterminada es mantener los archivos en línea y descargar archivos mientras los usas.

Para configurar OneDrive para descargar archivos solo cuando **** sea necesario, establezca la configuración Archivos a petición en Guardar espacio y descargar archivos mientras **los usa**. Para obtener más información, vea Consultar y establecer estados de archivos a petición en Windows .



NOTE

También puede repetir estos pasos para configurar un OneDrive personal, pero asegúrese de conservar el espacio de unidad y solo descargar archivos cuando los necesite.

SharePoint y Teams

SharePoint y Teams channel también se pueden sincronizar localmente con los dispositivos de escritorio, como portátiles y Surface Hubs, con el motor Sincronización de OneDrive móvil.

Para sincronizar los archivos corporativos internos con la unidad local con la Sincronización de OneDrive:

1. Vaya a un sitio SharePoint y vaya al directorio de documentos de nivel superior para ver o editar archivos que le interesan ver o editar desde el dispositivo local.
2. Seleccione el botón **Sincronizar** en la parte superior de la SharePoint cinta de opciones.
3. Seleccione en **Abrir** en el elemento emergente **Este sitio está intentando abrir Microsoft OneDrive**.
4. Compruebe que los SharePoint se sincronizan con la unidad local seleccionando en el icono OneDrive en la parte inferior derecha de la barra de tareas.
5. Compruebe que la configuración está configurada para mantener los archivos en línea y descargar los archivos solo cuando los use:
    a. Abra el explorador de archivos.
    b. Vaya a y haga clic con el botón secundario en SharePoint nombre; por ejemplo, **Contoso \ <SharePoint Document Folder Name> **.
    c. Seleccione **Liberar espacio**.
    d. La columna Estado mostrará el estado de los archivos y carpetas. Para obtener más información,

vea Sync SharePoint files with the Sincronización de OneDrive client .

6. Teams Los archivos de canal se almacenan en SharePoint sitios, con todas las mismas funciones SharePoint documentos, incluido el historial de versiones y la sincronización con los dispositivos de escritorio locales. Para sincronizar Teams de canal:

   a. Vaya al canal Teams de interés y seleccione la **pestaña** Archivos en la parte superior. A continuación, **seleccione Sincronizar**. Los archivos comenzarán a sincronizarse y estarán visibles en el Explorador de archivos en **Escritorio \ Contoso \ <name of the Teams Channel> **.

   b. Use el mismo procedimiento que usó para sincronizar sitios de SharePoint para mantener los archivos en la nube y descargarlos solo cuando los use, mantenga pulsado o haga clic con el botón secundario en el Explorador de archivos en el nombre del canal de Teams y, a continuación, seleccione Liberar espacio .

Surface Hub de lápiz

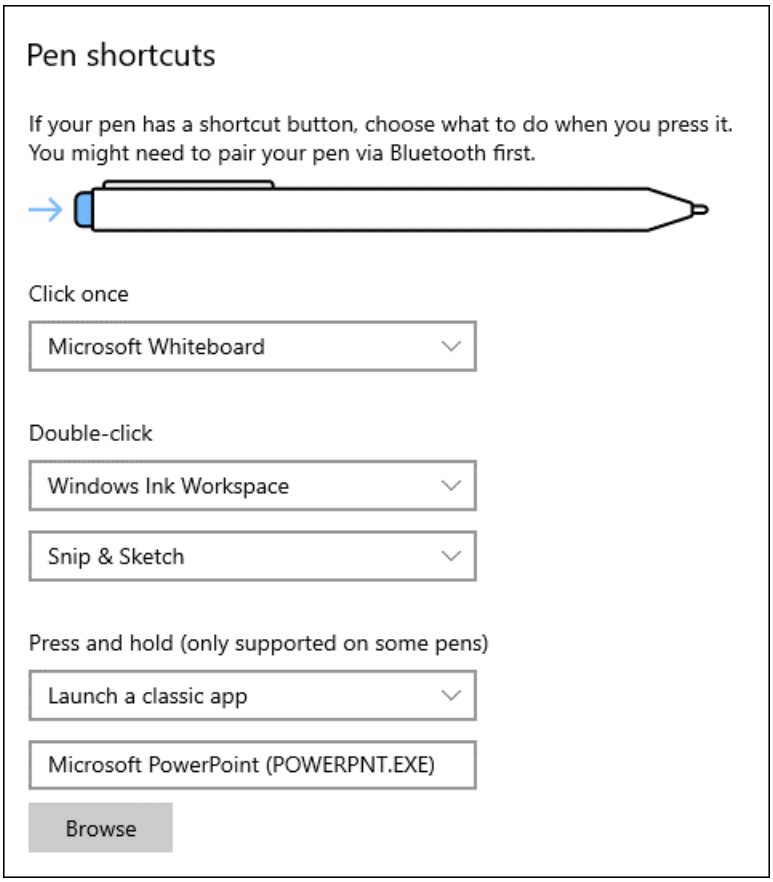
Emparejar el Bluetooth Surface Hub lápiz

Empareja el lápiz para mantener actualizado el firmware del lápiz, establecer los accesos directos del lápiz y obtener información de carga de batería en la página de configuración del dispositivo Bluetooth o en la aplicación Surface:

1. Seleccione **Iniciar** > **Configuración** > **dispositivos**.
2. Selecciona **Agregar Bluetooth u otro dispositivo**.
3. Elija **Bluetooth**.
4. Quite el botón de cola del lápiz y agite para desconectar la conexión de la batería.
5. Vuelva a colocar la tapa y mantenga presionada la tapa hasta que parpadee el LED de emparejamiento.
6. En la Surface Hub Bluetooth, elija **Surface Hub 2 pen**.
7. Complete la operación de emparejamiento.
8. Si el emparejamiento no se realiza correctamente, puede intentar emparejar el lápiz de nuevo. Si eso no funciona, puedes probar para ver si la batería se carga comprobando que el lápiz funciona en la aplicación Pizarra. Si no es así, reemplace la batería y vuelva a emparejar el lápiz. Si es necesario, reinicia el dispositivo y vuelve a intentarlo.

Establecer métodos abreviados de lápiz El Surface Hub tiene un botón de acceso directo que a veces se conoce como "clic de cola". La configuración de métodos abreviados requiere emparejar primero el lápiz, como se describió anteriormente.

1. Busque Pluma y seleccione **Pen & Windows Ink configuración**.
2. Cerca de la parte inferior de la página, seleccione Métodos abreviados de lápiz que abre el cuadro de diálogo, que se muestra aquí:



Configuración de cámara

Puedes montar la cámara en la parte superior o en cualquier lado del dispositivo. Monta la cámara en una posición para optimizar el ángulo de la cámara si estás usando el concentrador con un soporte de escritorio en lugar de un carro, o si estás cerca del concentrador. La cámara no gira automáticamente, por lo que debes tener una tecla hexadecimal de 2 mm para girar manualmente la cámara.

Para obtener más información sobre cómo montar de forma lateral la cámara y girar la cámara manualmente, consulte Surface Hub orientación del objetivo de la cámara 2S .

Windows Hello configuración

Surface Hub 2S que Windows 10 Enterprise permite el conjunto completo de aplicaciones de escritorio de Win32, así como opciones Windows Hello biométricas. El Surface Hub lector de huellas digitales 2 puede conectarse a cualquier puerto USB-C del dispositivo.

Para solicitar un lector de huellas digitales Surface Hub 2 o ver especificaciones técnicas, vea (surface-hub-2-essential-add-ons.md" target="_blank">Essential add-ons for Windows 10 Pro and Enterprise on Surface Hub 2 .

Después de insertar el **** lector de huellas digitales, seleccione Start > **Configuración** > **Accounts** > **Sign-in options**Windows Hello > **Fingerprint** para inscribir la huella digital.

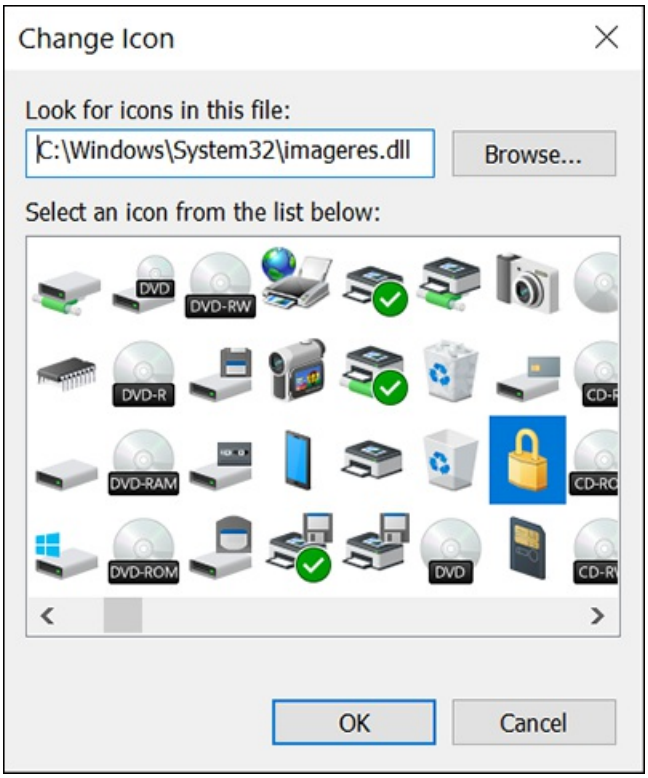
Usa un dispositivo Windows Hello certificado para el reconocimiento facial. La Surface Hub 2S no admite el reconocimiento Windows Hello rostro.

Habilitar un icono de acceso directo de pantalla de bloqueo en la barra de tareas

Para agregar un icono a la barra de tareas que habilita un bloqueo de pantalla táctil similar al método abreviado de teclado Windows-L:

1. Pulsa y mantén presionado o haz clic con el botón derecho en el escritorio, selecciona **Nuevo** > **acceso directo** > **Examinar** > **escritorio** > **Aceptar** > **siguiente**.
2. Proporcione un nombre para el acceso directo como **Bloquear mi PC**y, a continuación, seleccione **Finalizar**.
3. Haga clic con el botón secundario o pulse y mantenga presionado el acceso directo recién creado en el escritorio y seleccione **Propiedades**. En la **pestaña Acceso** directo, escriba lo siguiente en el **campo Destino: Rundll32.exe User32.dll,LockWorkStation**
4. Seleccione el **botón Cambiar icono** y vaya a **C:\Windows\System32\imageres.dll** y seleccione un icono para usar.

   Observa el siguiente ejemplo:



5. Seleccione **Aceptar** para guardar el acceso directo.
6. Haga clic con el botón secundario o pulse y mantenga presionado el acceso directo y seleccione **Anclar a la barra de tareas**.
7. Después de anclar el acceso directo de bloqueo a la barra de tareas, puede eliminarlo del escritorio.

Aplicaciones

Microsoft Whiteboard

Para instalar el Microsoft Whiteboard:

- Seleccione el **Área de trabajo de Windows Ink** en la parte inferior derecha de la barra de tareas y descargue **Whiteboard**.

Como alternativa, puede instalar whiteboard desde el Microsoft Store:

1. Abre Microsoft Store aplicación y busca **Whiteboard**.

2. Elige **No gracias para** iniciar sesión y usar en todos los dispositivos.
3. Anclar pizarra a la barra de tareas.

Aplicación Surface

1. En la Microsoft Store, busque **Surface**.
2. Establece el **filtro Disponible en** todos los **dispositivos**.
3. Instala la **aplicación Surface.** Esta debería ser la primera aplicación enumerada. Es posible que deba asociar la MSA a la Tienda para instalar la aplicación.
4. Anclar la **aplicación Surface** a la barra de tareas.

Recorte y anotación

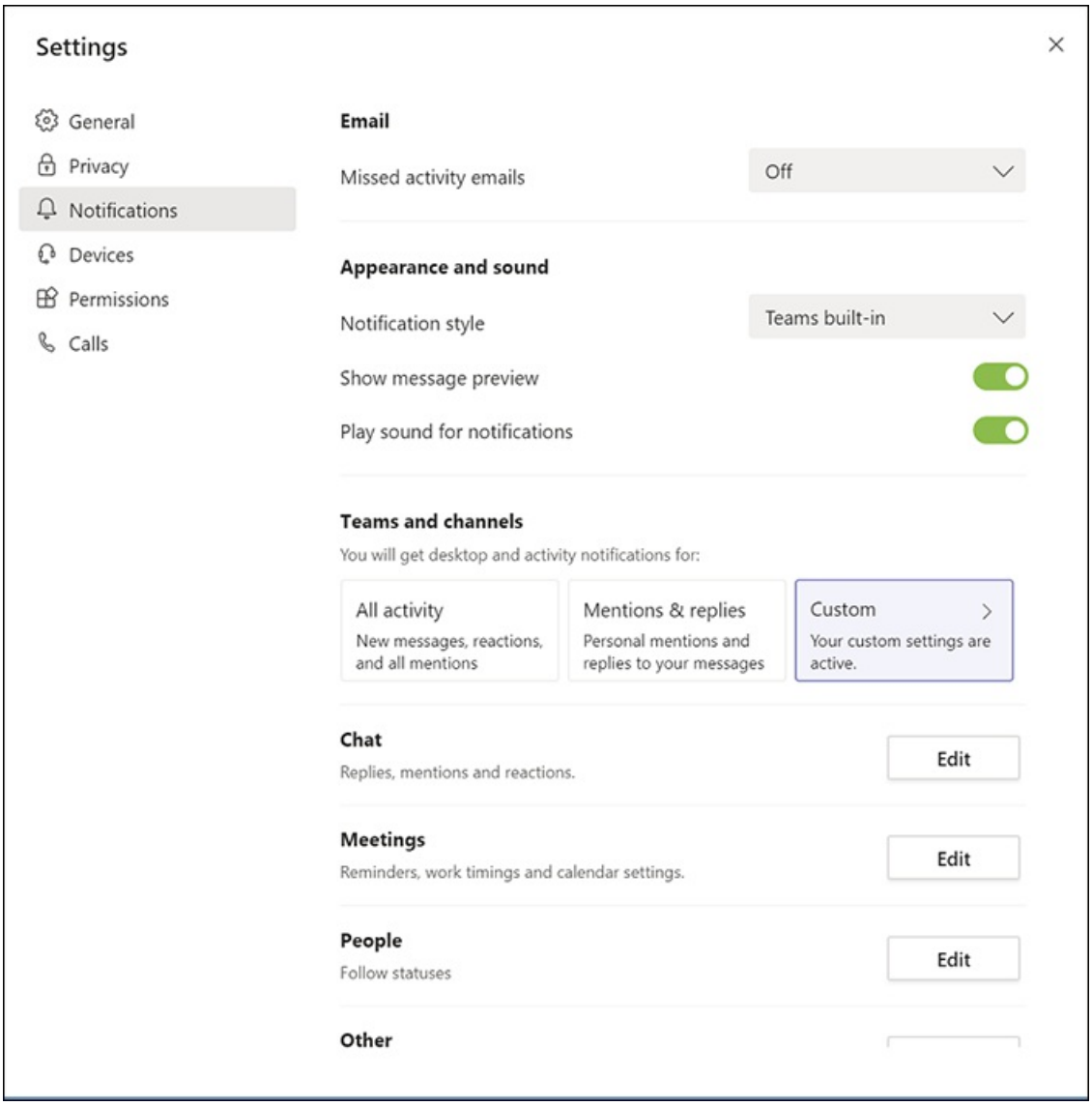
1. Abre la **aplicación Snip & Sketch** y anclarla a la barra de tareas.
2. Seleccione los puntos suspensivos en la esquina superior derecha y, a **continuación, seleccione Configuración**.
3. En **Configuración**, activa **Copia automática en el** Portapapeles , **Guardar snips** y **Varias ventanas** (opcional).

Microsoft Office

1. Abra el Office portal e instale las aplicaciones deseadas.
2. Anclar las Office deseadas a la barra de tareas.
3. Si Outlook está instalado, asegúrese de establecer la ost Outlook para guardar solo la memoria caché de las últimas dos semanas. Esto reducirá en gran medida el uso del disco y el tiempo de instalación.
   - Seleccione **Cuenta** > **de Configuración** y seleccione su cuenta.
   - Seleccione **Cambiar** y establezca el control deslizante para Usar el modo **Exchange caché** en 14 días.

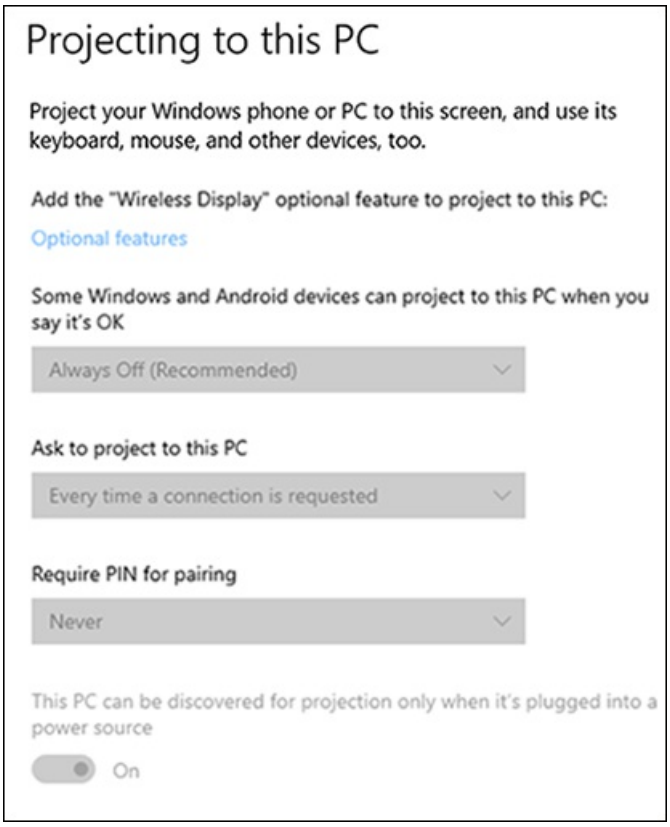
Microsoft Teams

1. Descargue e instale Microsoft Teams .
2. Configure las opciones para iniciar automáticamente la aplicación (opcional).
3. Anclar Teams a la barra de tareas.
4. Considera la posibilidad de Teams notificaciones en el dispositivo para evitar distracciones (opcional).



Conectar aplicación

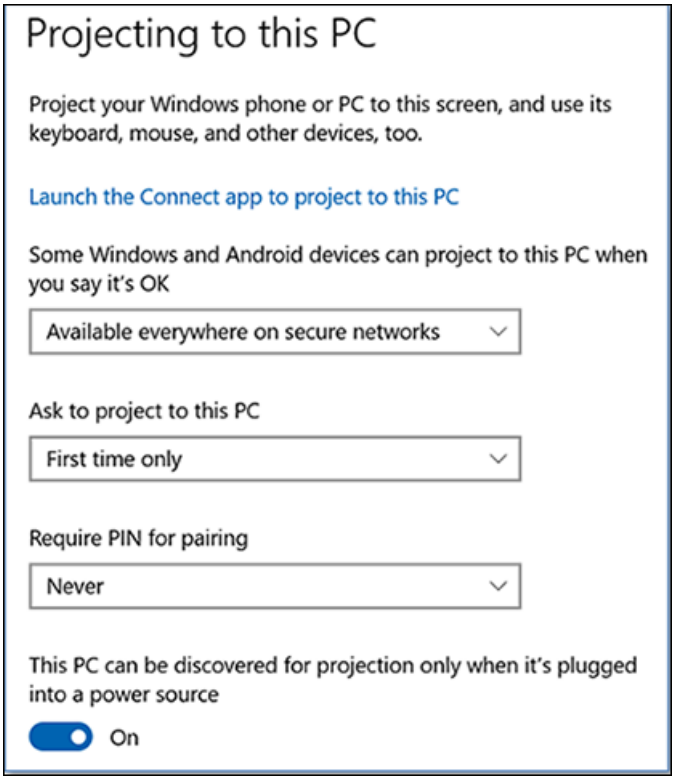
> **IMPORTANT**
>
> En Windows 10, versión 2004 y posteriores, la aplicación Conectar para la proyección inalámbrica mediante Miracast no está instalada de forma predeterminada, pero está disponible como una característica opcional. Si ha instalado (o actualizado a) Windows versión 2004 o posterior, puede ver lo siguiente en la pantalla Proyectar a este equipo en configuración:



1. Para instalar la aplicación desde la página de configuración ****"Proyectar a este equipo", selecciona Características opcionales Agregar una característica y, > **a** continuación, instala la **aplicación Pantalla** inalámbrica.
2. En **Algunos Windows y dispositivos Android**pueden proyectarse a este equipo cuando diga que está bien , elija:
   - **Disponible en todas** partes si el dispositivo no está en una red corporativa.
   - De lo contrario, **elija Disponible en todas partes en redes seguras.**
3. En **Solicitar proyecto a este equipo,** elija Solo primera **vez**.
4. En **Requerir PIN para el emparejamiento,** elija **Nunca**.
5. Para iniciar la aplicación y anclarla a la barra de tareas, busque **Conectar**.
6. Abre la aplicación. Mientras la aplicación está abierta, haz clic con el botón secundario en el icono Conectar de la aplicación en la barra de tareas y selecciona **Anclar a la barra de tareas.**
7. A continuación, cierra Conectar aplicación. **Project a este equipo** puede que no funcione a menos que la aplicación se haya ejecutado al menos una vez.

Configuración recomendada cuando no está en la red corporativa:

Configuración recomendada en la red corporativa:



<a name="your-phone">Tu Teléfono

La **Tu Teléfono** está instalada de forma predeterminada en Windows 10. Si no está presente, también puedes instalarlo desde Windows Store.

Para obtener información sobre cómo configurar la aplicación, consulta Cómo configurar Tu Teléfono en Windows 10 y sincronizar datos entre el equipo y el teléfono. Consulta también Cómo solucionar problemas comunes con Tu Teléfono aplicación en Windows 10 .

Zonas de lujo

Fancy Zones forma parte de una colección de herramientas denominada PowerToys en GitHub. Es una

excelente forma de usar la pantalla en un Surface Hub 2, ya que permite definir diseños fijos en la pantalla ("zonas") y, a continuación, seleccionar qué aplicación se ejecutará en cada zona.

El PowerToys wiki tiene instrucciones sobre cómo usar y personalizar cada herramienta, incluidos FancyZones. En un nivel alto: después de instalar PowerToys, puedes seleccionar o crear un diseño personalizado y, a continuación, mantener presionada la tecla mayús y arrastrar o usar teclas de teclado para mover una aplicación en ejecución a zonas específicas. El uso Bluetooth teclado y mouse USB te ayudarán con esto, o puedes usar el teclado táctil y el panel táctil en pantalla.

Sugerencias de power toys

- Para recibir notificaciones por correo electrónico PowerToys actualizaciones de lanzamiento en GitHub, haga clic en el botón "Registrarse" en la parte superior de la página.
- Una PowerToys se instala, puede recibir notificaciones de Windows o descargar e instalar las actualizaciones más **** recientes configurando la configuración de PowerToys Descargar actualizaciones automáticamente en on.
- Para llegar a la configuración de PowerToys, **** seleccione el quilate De arriba En ejecución de aplicaciones en la barra de tareas y, a continuación, haga clic con el botón secundario o presione y mantenga presionado el icono PowerToys hasta que aparezca el menú. Seleccione "Configuración".
- En la parte inferior de la página PowerToys configuración, activa **Descargar actualizaciones automáticamente.**
- Cuando se haya publicado una actualización, aparecerá Windows notificación que le dará la opción de cuándo instalar la actualización.

Explorador Chromium edge

Descargue e instale el nuevo explorador de Chromium edge .

Surface Hub Herramienta de diagnóstico de hardware

La Surface Hub de diagnóstico de hardware disponible de forma gratuita desde el Microsoft Store. La herramienta está diseñada para ayudarle a asegurarse de que su Surface Hub está funcionando en su mejor momento. Contiene pruebas para determinar si el firmware está actualizado y configurado correctamente. Las pruebas interactivas permiten confirmar que la funcionalidad esencial funciona según lo esperado. Si surgen problemas, los resultados se pueden guardar y compartir con el equipo de soporte técnico de SurfaceHub. Haga clic en el vínculo para instalarlo desde el Microsoft Store y, a continuación, anclar la aplicación a la barra de tareas.

Configuración adicional

Selección de cola de lápiz para iniciar pizarra

1. Busque Pluma y seleccione **Pen & Windows Ink configuración**.
2. Cerca de la parte inferior de la página, en **Métodos abreviados de lápiz,** establece **Seleccionar una vez** en **Microsoft Whiteboard**.

Administración de energía

Hay varias opciones de configuración de energía disponibles para obtener la mejor experiencia con Windows 10 Pro o Enterprise en Surface Hub 2. Esto incluye tiempos de espera de pantalla y equipo, y cómo interactúan con la detección de presencia humana integrada (Doppler), el protector de pantalla y la protección de contraseña y, si procede, cómo pasar la configuración de energía de directiva de grupo destinada a usuarios de equipos portátiles o de escritorio.

Windows 10 Pro o Enterprise en Surface Hub 2 impide que la pantalla duerma mediante acciones táctiles, de mouse y de teclado, así como la detección de ocupación humana integrada (Doppler). La detección de ocupación humana está habilitada de forma predeterminada, pero si se desea se puede deshabilitar en UEFI al alternar la

opción de dispositivo en la herramienta Configurador UEFI de Surface como parte de la migración inicial, o mediante la creación y aplicación de un paquete de configuración de UEFI posterior.

Administración de energía: configuración de suspensión de pantalla y equipo

1. Seleccione **Iniciar** > **Configuración** > **Power** > **& modo de suspensión**.
2. Establece el control deslizante del modo de energía en **Mejor rendimiento.**
3. Configure los valores de pantalla y suspensión según su preferencia, al tiempo que también tiene en cuenta la detección de presencia de Doppler que activa el dispositivo cuando se detecta el movimiento. Por lo tanto, como procedimiento recomendado, se recomienda establecer Pantalla en Desactivar después de **2** horas y el equipo desactivar después de **4 horas.**

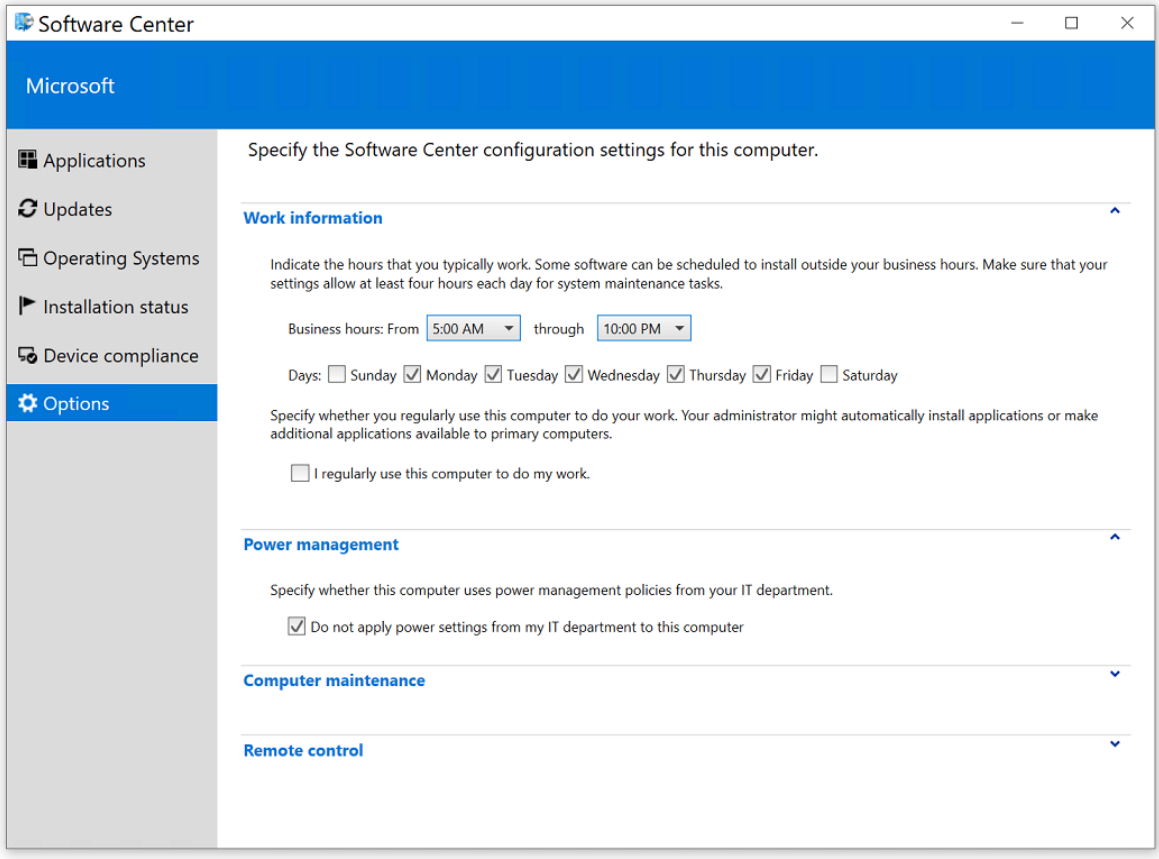
Administración de energía: protector de pantalla

1. Busque Pantalla **de bloqueo y** abra La configuración de pantalla de **bloqueo**.
2. Configure **la configuración de tiempo de espera de** pantalla y la configuración del **protector** de pantalla según sus preferencias. Los valores predeterminados recomendados son:
   - Protector de pantalla a (Ninguno) o un protector de pantalla de su elección.
   - Tiempo de espera a 15 minutos.
   - Al reanudar, muestra la pantalla de inicio de sesión.

Administración de energía: directiva de grupo

Antes de realizar el siguiente procedimiento, consulte con su departamento de TI para su aprobación para excluir un dispositivo Surface Hub 2S de la directiva global de administración de energía. Algunas opciones de configuración de administración de energía pueden deshabilitar la función de detección de presencia.

1. Busque el **Centro de software** y ábralo.
2. Seleccione **Opciones**.
3. Expanda Administración **de energía y** seleccione No aplicar la configuración de energía de mi departamento de TI a este **equipo**.



Sensor de almacenamiento

El Surface Hub 2 tiene una SSD de 128 GB para el almacenamiento local, por lo que es necesario tener en cuenta el uso de medidas de almacenamiento durante el uso normal. Para configurar Storage Sense:

1. Busque la **configuración de almacenamiento**, que se encuentra en Configuración del **sistema**.
2. En **Configuración**, seleccione Activar el sentido **de almacenamiento** para abrir la página **Storage** configuración.
3. Active Storage sense a **On**.
4. Seleccione **Configurar Storage Sense o** ejecutarlo ahora y configure la configuración para mantener los archivos en línea tanto como sea posible (debido a un espacio de unidad limitado).

Configuración recomendada:

- Ejecute Storage Sense = Todos los días.
- Eliminar archivos temporales que mis aplicaciones no usan = Cada 14 días (al menos).
- Elimine los archivos de la carpeta Descargas si han estado allí durante más de 30 días.
- OneDrive: el contenido se convertirá solo en línea si no se abre durante más de 30 días.

Modo tableta

Activa el modo tableta si lo deseas para las necesidades de accesibilidad.

Configuración de sonido

1. Busque la **configuración de sonidos** y abra esta página.
2. Seleccione **Panel de control de sonido** a la derecha y seleccione la **pestaña** Sonidos.
3. En **Eventos del** programa, establezca Device **Conectar y Device Disconnect** en **None**.

Notificaciones de silencio

1. Busque ayuda **de foco y** abra esta página.

2. Seleccione **Solo alarmas**. Esto evitará los control de control de notificaciones constantes.

Liberador de espacio en disco

1. Busca Limpieza **de disco** y abre esta aplicación.
2. En **Archivos para eliminar,** seleccione los archivos que desea eliminar.
3. También seleccione **Limpiar archivos del sistema.**

Completar y comprobar

1. Busque e instale todas las Windows actualizaciones.
2. Actualizar directiva de grupo.
   a. En un símbolo del sistema con privilegios elevados, escriba **gpupdate /force /boot /wait:0**.
3. Reinicia el dispositivo.
4. Compruebe las aplicaciones de la barra de tareas.
   - Conectar Aplicación
   - Icono de bloqueo
   - Recorte y anotación
   - Teams (si procede)
   - Office Aplicaciones (si procede)
   - Surface App
   - Pizarra
5. Compruebe la detección de presencia.
   - La detección de presencia será un icono verde en la bandeja del sistema.
6. Compruebe que la proyección a este equipo está habilitada con la Conectar app. Después de configurar Project configuración de **este equipo,** ejecute la aplicación Conectar al menos una vez. (Posteriormente, la Conectar app no necesita ejecutarse para poder proyectar a Surface Hub).
7. Compruebe la configuración de energía y suspensión.
   - Protector de pantalla: 15 minutos, establecido en (ninguno), Mystify o Blank; asegúrese de que la casilla de verificación para requerir contraseña está activada.
   - Pantalla: **Desactivar después de 2 horas**.
   - PC: **desactivar después de 4 horas**.
8. Compruebe Windows Hello funciona.
9. Compruebe que la sincronización de la configuración está deshabilitada.
10. Compruebe las aplicaciones de inicio.

> **TIP**
> Después de instalar y configurar Windows 10, el Surface Hub 2S se puede administrar como cualquier otro Windows 10 dispositivo.

Temas relacionados

Migrar a Windows 10 Pro o Enterprise en Surface Hub 2

Complementos esenciales para Windows 10 Pro y Enterprise en Surface Hub 2

12/01/2022 • 2 minutes to read

Si has migrado de Windows 10 Team a Windows 10 Pro o Enterprise en Surface Hub 2, puedes elegir entre una amplia variedad de accesorios que se conectan a través de USB-C, USB-A, HDMI o Bluetooth.

Surface Hub lector de huellas digitales 2

Si está ejecutando Windows 10 Pro o Windows 10 Enterprise en Surface Hub 2, puede iniciar sesión con el lector de huellas digitales Surface Hub 2 opcional, una opción de autenticación biométrica que usa Windows Hello.

Ordenar

Los clientes comerciales pueden realizar pedidos a través de sus revendedores de dispositivos autorizados de Surface.

Para usar Surface Hub lector de huellas digitales 2:

1. Inserte el lector de huellas digitales en cualquiera de los puertos de bisel USB C, ubicados en cada lado del dispositivo.
2. **Ir a Inicio** > **Configuración** > **Cuentas** > **Opciones de inicio de sesión** > **Windows Hello huella digital para** inscribir la huella digital.

Para obtener más información acerca de cómo configurar el lector de huellas digitales para que inicie sesión con Windows Hello, vea lo siguiente:

- Obtén más información sobre Windows Hello y cómo configurarlo.
- Windows Hello biometría en la empresa.

Tabla 1. Surface Hub 2 especificaciones técnicas del lector de huellas digitales

COMPONENTE	DESCRIPCIÓN
USB	Tipo DE USB personalizado C
Requisito del sistema	Windows 10 Pro, Windows 10 Enterprise.
Windows certificación	Windows 10
Tasa de aceptación falsa (FAR)	1/1,5 millones. FAR muestra la probabilidad de que un sistema de seguridad biométrica acepte incorrectamente los intentos de acceso de usuarios no autorizados.
Tasa de rechazo falso (FRR)	4.9%. FRR muestra la probabilidad de que un sistema de seguridad biométrica rechace incorrectamente los intentos de acceso de usuarios autorizados.

> **NOTE**
> Windows 10 Team, que se ejecuta en Surface Hub 2S no admite el Surface Hub 2 Lector de huellas digitales. Esto se debe a Windows 10 Team está diseñada para permitir que varios usuarios interactúen con el dispositivo en un entorno de sala de conferencias.

Windows Hello reconocimiento facial

Windows 10 Pro y Enterprise en Surface Hub 2 admite Windows Hello autenticación y requiere un accesorio de cámara Windows Hello certificado. Tenga en cuenta que la cámara integrada para Surface Hub 2S no está diseñada para la autenticación y no admite Windows Hello. Para obtener más información, vea Windows Hello.

Accesorios de audio y vídeo

Puedes ampliar las capacidades de audio y vídeo de Surface Hub 2 con periféricos de audio y cámara mediante los puertos USB-C o USB-A.

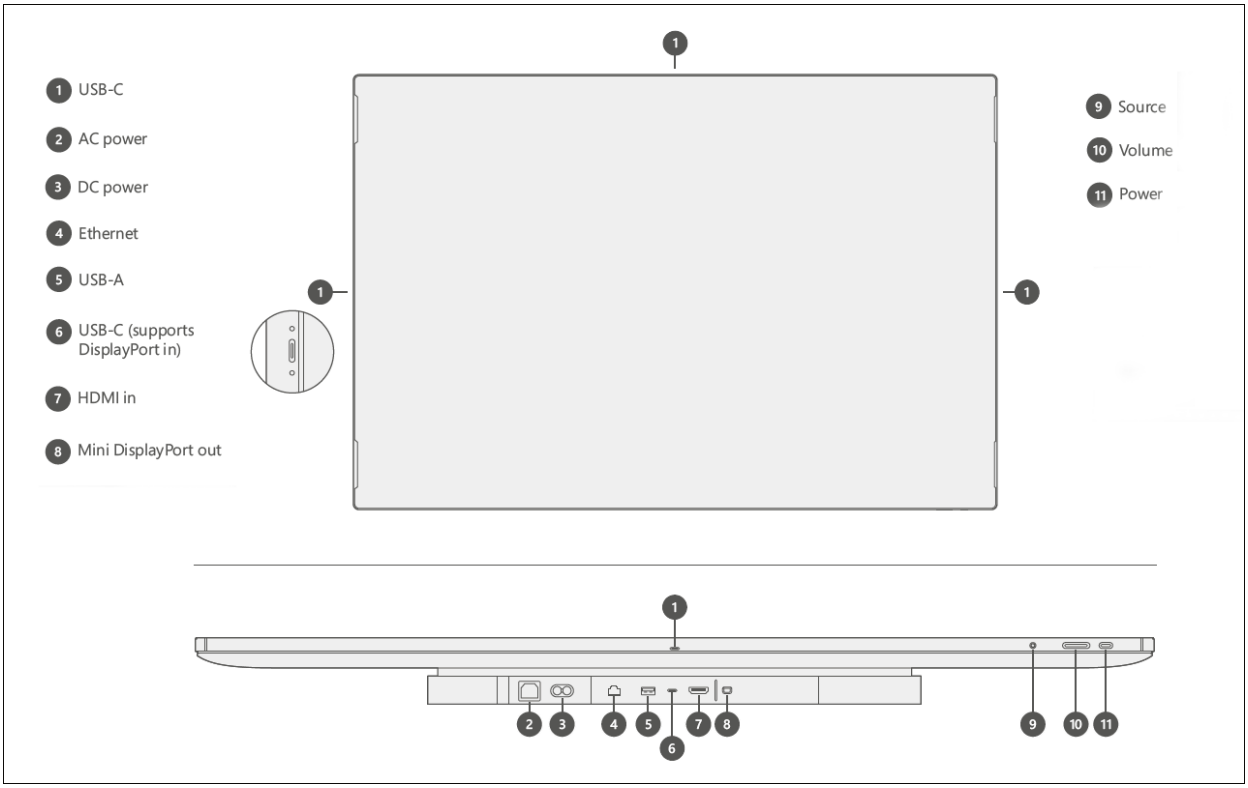
Para obtener información sobre los accesorios recomendados, vea:

- Dispositivos de audio y vídeo USB certificados para Microsoft Teams
- Teléfonos IP certificados para Microsoft Teams

Otros accesorios

Surface Hub 2 incluye los siguientes puertos para conectar una amplia variedad de dispositivos.

- 1 x puerto USB A en módulo de proceso (pantalla detrás)
- 4 x puertos USB C en biseles
- Bluetooth compatibilidad con 4.1
- HDMI 2.0



Para obtener más información, vea Surface Hub información general sobre los puertos 2S y el teclado

Obtén más información

- Configurar Windows 10 Pro o Enterprise en Surface Hub 2.

Salas de Microsoft Teams en Surface Hub

12/01/2022 • 3 minutes to read

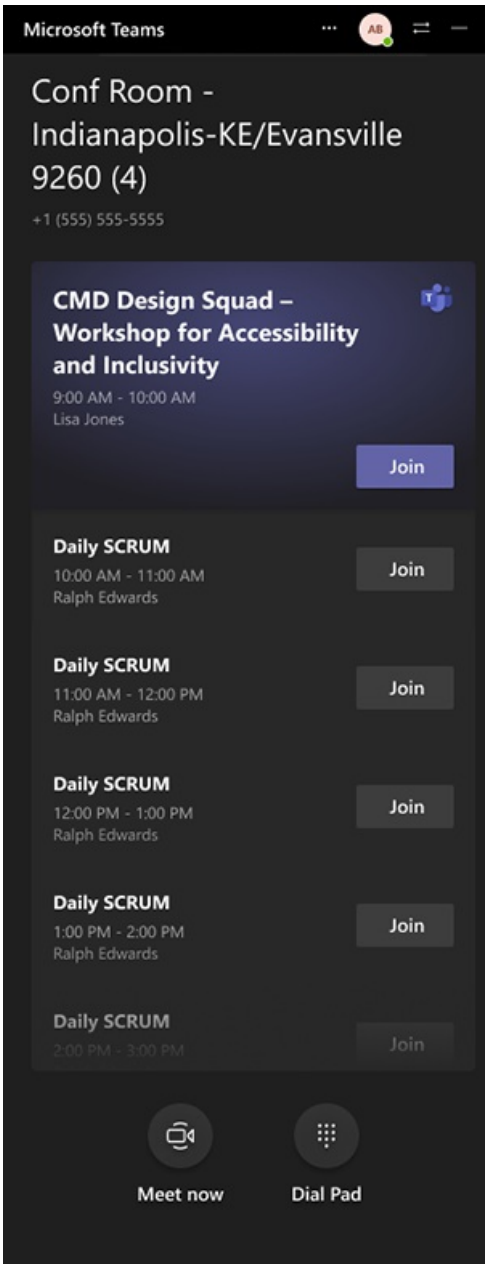
Salas de Teams para Surface Hub reemplaza automáticamente la aplicación Surface Hub Teams anterior tras la instalación de KB5004196, KB5004198 y KB5004199.

Novedades

- Las reuniones unidas desde la Surface Hub de bienvenida o la página Nueva agenda se unen a "Borde a borde" para poner a los usuarios en primer plano.
- Características de reunión conocidas, como burbujas de chat, reacciones, uso compartido de aplicaciones y escritorio, control y audio, soporte PowerPoint en directo, modo conjunto y galería grande.
- Salas de Teams en Surface Hub puede ejecutarse en paralelo con otras aplicaciones o ejecutarse minimizado.
- Los administradores pueden configurar características como reunión coordinada y unión de proximidad para Surface Hub. Los archivos XML son compatibles y se migrarán al nuevo modelo de configuración.
- Nuevas opciones de QoS y requisitos de red. Para obtener más información, vea Configure networking and Quality of Service for Microsoft Teams Room on Surface Hub.
- Si aún no es el valor predeterminado, Teams puede establecerse como **** la aplicación predeterminada para reuniones y llamadas en Configuración Surface Hub de & > **** > **audio**. Para obtener más información sobre los modos de reunión y configurarlos a través de la directiva MDM, consulta Administrar Surface Hub con un proveedor MDM.

En la experiencia de reunión

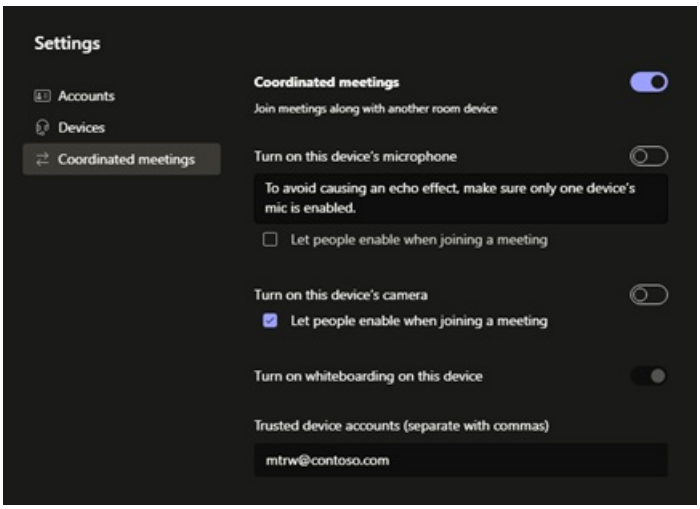
Salas de Teams en Surface Hub de reuniones está alineada con la experiencia familiar que los usuarios conocen desde sus dispositivos personales con los ajustes realizados para optimizar un dispositivo de pantalla grande. La Teams en Surface Hub permite a los usuarios acceder a características clave, como unirse a una reunión con un solo toque, Reunirse ahora y Panel de marcado para llamadas RTC o punto a punto.



Administrar Salas de Teams en Surface Hub

Puede personalizar la experiencia de Teams directamente desde el menú Configuración después de escribir las credenciales administrativas, incluidas:

- Configurar reuniones coordinadas y unión de proximidad.
- Ajusta la configuración de micrófonos, cámaras y altavoces predeterminados.
- Compruebe la versión del cliente y busque las actualizaciones más recientes.



La nueva Salas de Teams para Surface Hub cliente, aplicará automáticamente la configuración existente configurada a través de archivos XML, paquetes de aprovisionamiento o un proveedor mdm. Estos métodos, explicados en Administrar la configuración Microsoft Teams en Surface Hub, se reemplazarán por nuevas soluciones basadas en la nube, como se describe a continuación en Administración simplificada de Teamspróximamente Surface Hub .

Preparar las redes para Salas de Teams

Para optimizar Salas de Teams los requisitos y recomendaciones descritos en Configure networking and Quality of Service for Microsoft Teams Room on Surface Hub.

Administración simplificada de Teams que llega a Surface Hub

Cuando Salas de Teams para Surface Hub se publicó públicamente a finales de este año, los administradores pueden aprovechar las siguientes soluciones:

- **Teams Centro de administración.** Teams El Centro de administración proporciona una plataforma de autoadministrador completa para supervisar y administrar la experiencia Salas de Teams en Teams dispositivos. Teams El Centro de administración estará disponible para Salas de Microsoft Teams usuarios sin costo adicional.
- **Salas de Microsoft Teams servicio administrado.** El servicio administrado Salas de Microsoft Teams es un servicio de supervisión y administración de TI basado en la nube que mantiene los dispositivos Salas de Microsoft Teams y sus periféricos actualizados y supervisados proactivamente, lo que admite un entorno optimizado para una gran experiencia del usuario.

Compatibilidad con Salas de Teams en Government Community Cloud High (GCC-H)

Cuando Salas de Teams para Surface Hub se lanza públicamente a finales de este año, se necesita una actualización manual única del cliente a la versión 1.4.00.25354 para que pueda conectarse a un inquilino de GCC-H y, a continuación, mantenerse actualizado automáticamente:

- Confirme que el concentrador tiene kb5005611 o una actualización acumulativa Windows posterior instalada
- Usar Teams_Uninstall_win32.ppkg para quitar el Salas de Teams actual en Surface Hub versión

- Reiniciar el dispositivo
- Instalar Teams_win32.ppkg para instalar la versión 1.4.00.25354
- Reiniciar el dispositivo de nuevo

Pasos detallados:

1. Guarda ambos paquetes de aprovisionamiento en la raíz de la unidad USB.
2. Inserte la unidad USB en el Surface Hub.
3. En el Surface Hub, abra el menú Inicio, seleccione Todas las aplicaciones y, a continuación, seleccione Configuración.
4. Proporcione sus credenciales de administrador del concentrador cuando se le pida.
5. Ve a **Surface Hub**Administración de > **dispositivos**Agregar o quitar > **un paquete de aprovisionamiento**y, a continuación, **selecciona Agregar un paquete**.
6. En **Seleccionar un paquete,** seleccione el paquete de aprovisionamiento Teams_Uninstall_win32.ppkg y, a continuación, reinicie el Surface Hub.
7. En el Surface Hub, abra el menú Inicio, seleccione Todas las aplicaciones y, a continuación, seleccione Configuración.
8. Proporcione sus credenciales de administrador del concentrador cuando se le pida.
9. Ve a **Surface Hub**Administración de > **dispositivos**Agregar o quitar > **un paquete de aprovisionamiento**y, a continuación, **selecciona Agregar un paquete**.
10. En **Seleccionar un paquete,** seleccione el paquete de aprovisionamiento Teams_win32.ppkg y, a continuación, reinicie el Surface Hub.

Configurar las redes y la calidad del servicio para Salas de Microsoft Teams en Surface Hub

12/01/2022 • 2 minutes to read

En este artículo se explica cómo preparar el entorno para optimizar los Salas de Microsoft Teams en Surface Hub.

Crear y probar una cuenta de dispositivo

Una cuenta de dispositivo es una cuenta que el Salas de Microsoft Teams usa para tener acceso a las características desde Exchange, como el calendario, y para habilitar Skype Empresarial. Consulta Crear y probar una cuenta de dispositivo

Comprobar la disponibilidad de la red

> **TIP**
> Se recomienda encarecidamente usar los procedimientos para la configuración de red enumerados en Microsoft 365 principios de conectividad de red

Salas de Teams en Surface Hub debe tener acceso a una red que cumpla estos requisitos:

- Acceso a la instancia de Active Directory Azure Active Directory (Azure AD)
- Acceso a un servidor que puede proporcionar una dirección IP mediante DHCP. Salas de Microsoft Teams en Surface Hub no se puede configurar con una dirección IP estática.
- Acceso a los puertos HTTP 80 y 443.
- Puertos TCP y UDP configurados como se describe en Requisitos de puerto y protocolo para Microsoft 365 y Office 365 direcciones URL e intervalos de direcciones IP para Microsoft Teams.

> **IMPORTANT**
> Salas de Microsoft Teams no admite la autenticación de proxy, ya que puede interferir con las operaciones regulares de Teams. Asegúrese de que Surface Hub dispositivos o Microsoft 365 de servicio de Microsoft 365 se han exento de la autenticación de proxy antes de entrar en producción con Salas de Teams en Surface Hub.

Implementar calidad de servicio (QoS) en Surface Hub

Calidad de servicio (QoS) es una combinación de tecnologías de red que permite a los administradores optimizar la experiencia de comunicaciones de uso compartido de aplicaciones y audio en tiempo real. La configuración de QoS para Microsoft Teams en el Surface Hub puede realizarse con el proveedor de administración de dispositivos móviles (MDM) o a través de un paquete de aprovisionamiento.

Para configurar QoS para Surface Hub con Microsoft Intune:

1. En Intune, cree una directiva personalizada.
2. En **Custom OMA-URI Configuración**, seleccione **Agregar**. Para cada configuración que agregue, escribirá un nombre, una descripción (opcional), un tipo de datos, OMA-URI y un valor.

3. Para garantizar una calidad óptima de vídeo y audio en Surface Hub, agrega la siguiente configuración de QoS al dispositivo.

NOMBRE	DESCRIPCIÓN	OMA-URI	TIPO	VALOR
Puertos de audio	Rango de puertos de audio	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsAudio/SourcePortMatchCondition	Cadena	50000-50019
DSCP de audio	Marcado de puertos de audio	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsAudio/DSCPAction	Integer	46
Puerto de vídeo	Rango de puertos de vídeo	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsVideo/SourcePortMatchCondition	Cadena	50020-50039
DSCP de vídeo	Marcado de puertos de vídeo	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsVideo/DSCPAction	Integer	34
Puerto compartido	Intervalo de puertos compartidos	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsSharing/SourcePortMatchCondition	Cadena	50040-50059
Uso compartido de DSCP	Marcado de puertos compartidos	./Device/Vendor/MSFT/NetworkQoSPolicy/TeamsSharing/DSCPAction	Integer	18

4. Cuando se haya creado la directiva, impleméntela en Surface Hub.

Obtén más información

- Implementar calidad de servicio (QoS) en Microsoft Teams

Aplicación de Microsoft Teams para Surface Hub

12/01/2022 • 2 minutes to read

La aplicación de Microsoft Teams para Surface Hub se actualiza periódicamente y está disponible a través de Microsoft Store. Si administras Surface Hub con actualizaciones automáticas habilitadas (configuración predeterminada), la aplicación se actualizará automáticamente.

Historial de versiones

VERSIÓN DE LA APLICACIÓN DE LA TIENDA	ACTUALIZACIONES	PUBLICADO EN MICROSOFT STORE
0.2020.84.19701	- Reuniones coordinadas de Teams con salas de Microsoft Teams - Unión a reuniones basadas en proximidad	12 de agosto de 2020
0.2020.521.2344.0	- Vista Galería 3x3 en Surface Hub - Capacidad para buscar usuarios externos	10 de junio de 2020
0.2020.13201	- Mejoras de calidad y correcciones de errores	1 de junio de 2020
0.2020.4301.0	- Aceptar llamadas RTC entrantes en Surface Hub - Consum Attendee/Presenter role changes	21 de mayo de 2020

Más información

- Administrar la configuración de Microsoft Teams en Surface Hub

Accesorios de audio y vídeo certificados de Microsoft Teams para Surface Hub 2S

12/01/2022 • 2 minutes to read

Surface Hub modelos de 2S de 50" y 85" están certificados para Microsoft Teams para 2,3 metros como un dispositivo todo en uno en espacios de colaboración y acurrucación. La familia Surface Hub 2S se puede extender a salas más grandes con los siguientes periféricos certificados de Microsoft Teams probados y aprobados que sacan el máximo partido de cualquier espacio cuando se combinan con Surface Hub 2S de 50" y 85".

Microsoft Teams de audio certificados

MODELO	DESCRIPCIÓN
Yamaha YVC-1000MS	Para un máximo de seis participantes. - Use de uno a cinco micrófonos de expansión Microsoft Teams certificación en salas con hasta 40 participantes.
Sennheiser EXPAND SP 20	Para un máximo de seis participantes. Microsoft Teams certificado.
Yealink CP900	Para un máximo de seis participantes. Microsoft Teams certificado.

Microsoft Teams de vídeo certificados

MODELO	DESCRIPCIÓN
Jabra PanaCast	4K, 180 grados. Hasta 3 metros para sujetos de vídeo
Poly Studio: barra de vídeo USB de la sala de huddle	4K, 120 grados Hasta 3,7 metros para sujetos de audio y vídeo
Polycom EagleEye Director II	1080p, 65 grados Salas medianas de más de 10 participantes
Logitech Rally Bar	4K, 90 grados, PTZ, control manual/digital, USB 3.0 Type-C, privacy assurance

Obtén más información

- Sala de reuniones Sistemas, teléfonos VoIP, auriculares | Microsoft Teams

Conectar dispositivos a Surface Hub 2S

12/01/2022 • 6 minutes to read

Surface Hub 2S le permite conectar dispositivos externos, reflejar la pantalla en Surface Hub 2S a otro dispositivo y conectar varios periféricos de terceros, como cámaras de videoconferencia, teléfonos de conferencia y dispositivos de sistema Room.

Puedes mostrar el contenido de tus dispositivos a Surface Hub 2S. Si el dispositivo de origen está basado en Windows, ese dispositivo también puede proporcionar TouchBack y InkBack, que toma vídeo y audio del dispositivo conectado y los presenta en Surface Hub 2S. Si Surface Hub 2S encuentra una señal de protección de contenido digital (HDCP) de ancho de banda alto, como un reproductor de DVD Blu-Ray, el origen se muestra como una imagen en negro.

> **NOTE**
> Surface Hub 2S usa la entrada de video seleccionada hasta que se establece una nueva conexión, se interrumpe la conexión existente o se cierra la aplicación Connect.

Configuraciones cableadas recomendadas

En general, se recomienda usar conexiones de cable nativas siempre que sea posible, como USB-C o USB-C o HDMI a HDMI. Otras combinaciones, como MiniDP a HDMI o MiniDP a USB-C también funcionan. Es posible que se necesite una configuración adicional para optimizar la experiencia de salida del video, tal y como se describe en esta página.

CONEXIÓN	FUNCIONALIDAD	DESCRIPCIÓN
HDMI + USB-C	HDMI-in para audio y vídeo USB-C para TouchBack y InkBack	USB-C admite TouchBack y InkBack con la conexión A/V HDMI. Use USB-C para USB-A para conectarse a equipos heredados. **Nota:** Para obtener los mejores resultados, conecta HDMI antes de conectar un cable USB-C. Si el equipo que usas para HDMI no es compatible con TouchBack y InkBack, no necesitarás un cable USB-C.
USB-C (mediante módulo de cálculo)	Vídeo: en vídeo Audio en	Cable único necesario para A/V TouchBack y InkBack son compatibles HDCP habilitado
HDMI (en Puerto)	Vídeo, audio en Surface Hub 2S	Cable único necesario para A/V TouchBack y InkBack no compatibles HDCP habilitado

CONEXIÓN	FUNCIONALIDAD	DESCRIPCIÓN
Salida de MiniDP 1,2	Vídeo: salida, como el reflejo a un proyector más grande.	Cable único necesario para A/V

Al conectar un equipo invitado a Surface Hub 2S a través del puerto USB-C, se descubren y configuran varios dispositivos USB. Estos dispositivos periféricos se crean para TouchBack y InkBack. Como se muestra en la tabla siguiente, los dispositivos periféricos se pueden ver en el administrador de dispositivos, que mostrará nombres duplicados para algunos dispositivos, como se muestra en la tabla siguiente.

PERIFÉRICOS	LISTADO EN EL ADMINISTRADOR DE DISPOSITIVOS
Dispositivos de interfaz humana (HID)	Dispositivo de control del consumidor compatible con HID Lápiz compatible con HID Lápiz compatible con HID (elemento duplicado) Lápiz compatible con HID (elemento duplicado) Pantalla táctil compatible con HID Dispositivo de entrada USB Dispositivo de entrada USB (elemento duplicado)
Teclados	Teclado PS/2 estándar
Mouse y otros dispositivos señaladores	Mouse compatible con HID
Controladores USB	Concentrador USB genérico Dispositivo compuesto USB

Conexión de vídeo en Surface Hub 2S

Puedes introducir video en Surface Hub 2S con USB-C o HDMI, como se indica en la tabla siguiente.

Configuración de vídeo de Surface Hub 2S

TIPO DE SEÑAL	RESOLUCIÓN	VELOCIDAD DE FOTOGRAMAS	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	0,30	X	X
HDTV	720p	60	X	X
HDTV	1080p	60	X	X
4K UHD	3840x2560	0,30	X	X

> **NOTE**
> La resolución de 4K UHD (3840 × 2560) solo se admite al conectarse a puertos en el módulo de cálculo. No es compatible con los puertos USB "de invitado" que se encuentran en los lados izquierdo, superior y derecho del dispositivo.

> **NOTE**
> Es posible que el video de un PC externo conectado aparezca más pequeño cuando se muestra en Surface Hub 2S.

Reflejar la pantalla de 2.

Puede enviar video a otra pantalla con MiniDP, como se indica en la tabla siguiente.

Configuración de salida de video de Surface Hub 2S

TIPO DE SEÑAL	RESOLUCIÓN	VELOCIDAD DE FOTOGRAMAS	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 incluye un puerto de salida de video de MiniDP para proyectar contenido visual desde Surface Hub 2S a otra pantalla. Si tiene previsto usar Surface Hub 2S para proyectar en otra pantalla, tenga en cuenta las siguientes recomendaciones:

- **Teclado requerido.** Antes de empezar, deberás conectar un teclado externo con cable o Bluetooth a Surface Hub 2S. Ten en cuenta que, a diferencia de la Surface Hub original, un teclado para Surface Hub 2S se vende por separado y no se incluye en el paquete de envío.

- **Establecer el modo duplicado.** Surface Hub 2S admite vídeo: solo en modo duplicado. Sin embargo, aún tendrá que configurar manualmente el modo de presentación cuando se conecte por primera vez:
  1. Escriba la **tecla del logotipo de Windows** + **P**, que abre el panel del proyecto en el lado derecho de Surface Hub 2s y, a continuación, seleccione **duplicar** modo.
  2. Cuando haya terminado con la sesión de Surface Hub 2S, seleccione **finalizar sesión**. Esto garantiza que la configuración duplicada se guardará para la siguiente sesión.

- **Planear diferentes relaciones de aspecto.** Al igual que otros dispositivos de Surface, Surface Hub 2S usa una relación de aspecto de 3:2 (la relación entre el ancho y el alto de la pantalla). La proyección de Surface Hub 2 en pantallas con diferentes relaciones de aspecto es compatible. Sin embargo, ten en cuenta que, dado

que Surface Hub 2 duplica la pantalla, la salida de MiniDP también se muestra solo en una relación de aspecto 3:2, lo que puede dar lugar a una panorámica o a una cortina en función de la relación de aspecto de la pantalla de recepción.

> **NOTE**
> Si su segundo monitor usa una relación de aspecto de 16:9 (la relación predominante para la mayoría de los monitores de TV), es posible que aparezcan barras negras a la izquierda y a la derecha de la pantalla reflejada. Si esto sucede, es posible que desee informar a los usuarios de que no es necesario ajustar la segunda pantalla.

Selección de cables

Tenga en cuenta las siguientes recomendaciones:

- **USB.** Cables USB 3,1 Gen 2.
- **MiniDP.** Cables de DisplayPort certificados para un máximo de 3 metros de longitud.
- **HDMI.** Si se necesita un cable largo, se recomienda usar HDMI debido a la amplia disponibilidad de los cables de largo alcance y rentable con la capacidad de instalar repetidores si es necesario.

> **NOTE**
> La mayoría de los orígenes de DisplayPort cambiarán automáticamente a la señalización HDMI si se detecta HDMI.

Conexión inalámbrica a Surface Hub 2S

Windows 10 es compatible de forma nativa con Miracast, que te permite conectarte a Surface Hub 2S.

Para conectar con Miracast:

1. En el dispositivo Windows 10, escriba la **tecla del logotipo de Windows + K**.
2. En la ventana de conexión, busca el nombre de tu Surface Hub 2 en la lista de dispositivos cercanos. Puede encontrar el nombre de su Surface Hub 2 en la esquina inferior izquierda de la pantalla.
3. Escribe un PIN si el administrador del sistema ha habilitado la configuración del PIN para las conexiones Miracast. Para ello, debes introducir un número PIN cuando te conectes a Surface Hub 2S por primera vez.

> **NOTE**
> Si no ve el nombre del dispositivo Surface Hub 2S de la forma esperada, es posible que la sesión anterior se haya cerrado prematuramente. Si es así, inicie sesión en Surface Hub 2S directamente para finalizar la sesión anterior y, a continuación, conéctese desde el dispositivo externo.

Conexión de periféricos a Surface Hub 2S

Accesorios Bluetooth

Puede conectar los siguientes accesorios a Surface Hub-2 con Bluetooth:

- Ratones
- Teclados
- Auriculares
- Altavoces
- Surface Hub 2 plumas

NOTE

Tras conectar unos auriculares o un altavoz Bluetooth, es posible que debas cambiar la configuración predeterminada de micrófono y altavoces. Para obtener más información, vea **Administración local para la configuración de Surface Hub**.

Instalar la actualización 2020 de Windows10Team

12/01/2022 • 2 minutes to read

El nuevo sistema operativo Surface Hub, **Windows 10 Team 2020 Update,** basado en Windows 10 versión 20H2, ya está disponible para Surface Hub 2S y el Surface Hub original (v1).

- Vea también: Problemas conocidos: Windows 10 Team 2020 Update

Distribución

Puedes obtener Windows 2020 Update con uno de los siguientes métodos:

- **Windows Update para empresas**.
- **Imagen de recuperación completa de metal (BMR).** Opción recomendada para los clientes que unen sus dispositivos a Azure Active Directory o no permiten que sus dispositivos reciban actualizaciones de Internet. Para empezar, consulta Descargar una imagen de recuperación para Surface.
- **Windows Update.** La disponibilidad varía según la región o el país, como se indica en la tabla siguiente:

FASE	PAÍS/REGIÓN	INICIO
1	NZ, Australia, Canadá, Bélgica, México	Octubre de 2020
2	Reino Unido, Japón, Suiza, Italia	Noviembre de 2020
3	Alemania, Países Bajos	Finales de febrero de 2021
4	Global	Principios de marzo de 2021

Mantenimiento de Surface Hubs con Windows 10 Team Edition versión 1703

El soporte técnico completo para Windows 10 Team Edition versión 1703 está programado para continuar hasta el 16 de marzo de 2021.

Dispositivos 2S

Los clientes de todas las regiones pueden actualizar sus dispositivos Surface Hub 2S a la actualización de 2020 a través de Windows Update, Windows Update para empresas o mediante la imagen de recuperación completa (BMR), como se explica en Reset and recovery for Surface Hub 2S.

Dispositivos V1

Los clientes de todas las regiones pueden actualizar sus dispositivos Surface Hub v1 a 2020 Update a través de Windows Update, Windows Update para empresas o mediante la Herramienta de recuperación de Surface Hub. KB5000749 debe instalarse para recibir la actualización por aire. Para obtener más información, consulta Blog de Surface IT Pro.

Novedades

Windows 10 Team 2020 Update ofrece mejoras importantes en la implementación y la facilidad de administración de dispositivos, junto con las características más recientes de Windows 10. Para obtener más información, consulta Novedades de Windows 10 Team 2020 Update.

Antes de comenzar

Antes de instalar Windows 10 Team 2020 Update, asegúrate de guardar la clave de BitLocker asociada al dispositivo.

Para guardar manualmente la clave de BitLocker

1. Inserta una unidad USB en Surface Hub.
2. En Surface Hub, abre **Configuración** y escribe tus credenciales de administrador cuando se te pida.
3. Vaya a **Actualizar &** > **recuperación de seguridad**.
4. En **BitLocker,** seleccione **Guardar**. La clave BitLocker se guarda en un archivo de texto en la unidad USB.

Para obtener más información, consulta Guardar la clave de BitLocker.

Más información

- Novedades de la actualización Windows10 Team 2020
- Actualización al lanzamiento de Windows 10 Team

Problemas conocidos: Surface Hub

12/01/2022 • 4 minutes to read

En este artículo se enumeran los problemas conocidos para Surface Hubs que ejecutan el sistema operativo actual, Windows 10 Team 2020 Update.

Para asegurarse de Surface Hub recibe las actualizaciones más recientes, **** inicie sesión con una cuenta de administrador y seleccione Todas las aplicaciones Configuración Actualización y seguridad Windows Actualización y, a continuación, instale todas las > **** > **** > **** actualizaciones.

PROBLEMA	DESCRIPCIÓN	SOLUCIÓN
Al usar la aplicación pizarra en Surface Hub dispositivos, el contenido no se puede compartir por correo electrónico.	Al pasar por el flujo de exportación de pizarra para enviar por correo electrónico el contenido de la aplicación pizarra, Surface Hub dispositivos están mostrando actualmente "El dispositivo no está configurado para correo electrónico". Como resultado, el contenido de la pizarra no se puede compartir por correo electrónico.	Microsoft conoce y está investigando activamente este problema. Microsoft proporcionará información adicional sobre una resolución lo antes posible.
Algunos Surface Hubs están experimentando problemas de conectividad con sus áreas de trabajo de Azure Log Analytics (anteriormente conocidas como OMS).	Para los dispositivos Surface Hub afectados, al usar Azure Monitor, no se notifica ningún dato al área de trabajo.	Microsoft conoce y está investigando activamente este problema. Microsoft proporcionará información adicional sobre una resolución lo antes posible.
Algunos Surface Hubs se reinician cuando un usuario selecciona "Finalizar sesión".	Cuando Surface Hub usuarios del dispositivo seleccionan la funcionalidad "Finalizar sesión" para borrar los datos de usuario, el dispositivo Surface Hub puede detectar erróneamente un error de limpieza, lo que obliga a reiniciar Windows para garantizar que la limpieza se realiza correctamente.	Microsoft conoce y está investigando activamente este problema. Microsoft proporcionará información adicional sobre una resolución lo antes posible.
Algunos Surface Hubs pueden dejar de sincronizar el reloj de su equipo con time.windows.com si han estado afiliados a Azure Active Directory o configurados sin ninguna filiación. Cuando esta sincronización no funciona, el tiempo en el dispositivo puede desviar de la hora real.	La desviación del reloj más allá de 5 minutos puede provocar errores de autenticación en escenarios Surface Hub estándar, incluido Teams inicio de sesión.	En el dispositivo afectado, ve a **Todas**las aplicaciones Configuración Hora & idioma Fecha & hora y desactiva Establecer hora automáticamente y vuelve > **** > **a** > **** activar. **** Microsoft también está investigando activamente este problema y proporcionará información adicional sobre una resolución lo antes posible.
La configuración de calidad de servicio (QoS) no funciona como se esperaba	Después de configurar la configuración de QoS a través de la directiva MDM o el paquete de aprovisionamiento, las marcas DSCP no se aplican al tráfico multimedia Teams o Skype Empresarial (SfB).	Microsoft conoce y está investigando activamente este problema. Microsoft proporcionará información adicional sobre una resolución lo antes posible.

PROBLEMA	DESCRIPCIÓN	SOLUCIÓN
Se produce un error en la sincronización de calendario de cuentas de dispositivo híbrida con buzones locales.	Surface Hub dispositivos usan de forma predeterminada la autenticación moderna para cuentas que existen en Azure AD, incluso si tienen buzones locales que no funcionan con esta característica. En este escenario, Exchange deja de sincronizar reuniones con el dispositivo. Como resultado, el dispositivo no recibe ni muestra nuevas reuniones.	Después de instalar KB4598291 (o un Windows CU posterior), el CSP de SurfaceHub tiene un nuevo parámetro ExchangeModernAuthEnabled disponible para alternar el uso de la autenticación moderna. Esto se puede establecer en false a través de la directiva MDM o el paquete de aprovisionamiento para evitar que el concentrador use la autenticación moderna.
Un pequeño subconjunto de dispositivos Surface Hub v1 no pueden actualizar automáticamente a la actualización Windows 10 Team 2020.	Este pequeño subconjunto de dispositivos Surface Hub v1 están en un estado que impide la compatibilidad con la actualización directa a través de Windows Update.	Vuelva a crear manualmente la imagen del dispositivo en la Windows 10 Team 2020 Update con la herramienta Surface Hub recuperación.
Surface Hub muestra el mensaje "Ningún dispositivo de arranque" después de intentar instalar la actualización Windows 10 Team 2020.	Durante el Windows update para Windows 10 Team 2020, algunos dispositivos Hub v1 pasarán a un estado no arrancable.	Vuelva a crear manualmente la imagen del dispositivo en la Windows 10 Team 2020 Update con la herramienta Surface Hub recuperación.
Los dispositivos hub 2S no pueden recibir actualizaciones de controladores con WSUS.	Surface Hub 2S admite Windows Update y Windows Update para empresas para distribuir controladores; no se admite Windows Server Update Services (WSUS).	Si usa WSUS, migre a Windows Update for Business. **Más información:** ¿Qué es Windows actualización para empresas?
El Centro de acciones tiene un vínculo de Configuración no se puede hacer clic.	Este vínculo no debe aparecer en Windows 10 Team y puede causar confusión.	La funcionalidad es la misma que antes de la actualización de 2020; la sección Aplicaciones de la menú Inicio debe usarse para iniciar la Configuración aplicación.

Configurar cuentas de administrador no globales en Surface Hub

12/01/2022 • 4 minutes to read

La actualización de Windows 10 Team 2020 agrega compatibilidad para configurar cuentas de administrador no globales que limiten los permisos a la administración de la aplicación Configuración en dispositivos Surface Hub unidos a un dominio de Azure AD. Esto le permite tener en cuenta los permisos de administración Surface Hub y evitar el acceso de administrador potencialmente no deseado en todo un dominio de Azure AD. Antes de comenzar, asegúrese de que el Surface Hub está unido a Azure AD e Intune autoinscribirse. Si no es así, tendrá que restablecer Surface Hub y completar el programa de instalación de la primera vez y sin necesidad de usar (OOBE), eligiendo la opción de unirse a Azure AD.

Resumen

El proceso de creación de cuentas de administración no globales implica los siguientes pasos:

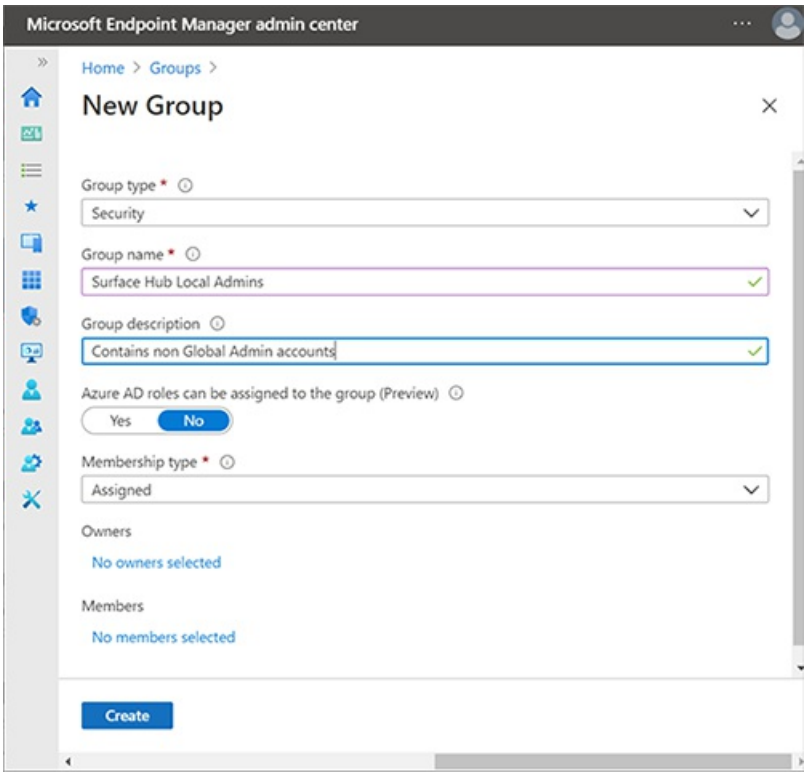
1. En Microsoft Intune, cree un grupo de seguridad que contenga los administradores designados para administrar Surface Hub.
2. Obtener SID de grupo de Azure AD con PowerShell.
3. Cree un archivo XML que contenga sid de grupo de Azure AD.
4. Cree un grupo de seguridad que contenga los Surface Hub que administrará el grupo seguridad de administradores no globales.
5. Crea un perfil de configuración personalizado destinado al grupo de seguridad que contiene los Surface Hub dispositivos.

Crear grupos de seguridad de Azure AD

En primer lugar, cree un grupo de seguridad que contenga las cuentas de administrador. A continuación, cree otro grupo de seguridad para Surface Hub dispositivos.

Crear grupo de seguridad para cuentas de administrador

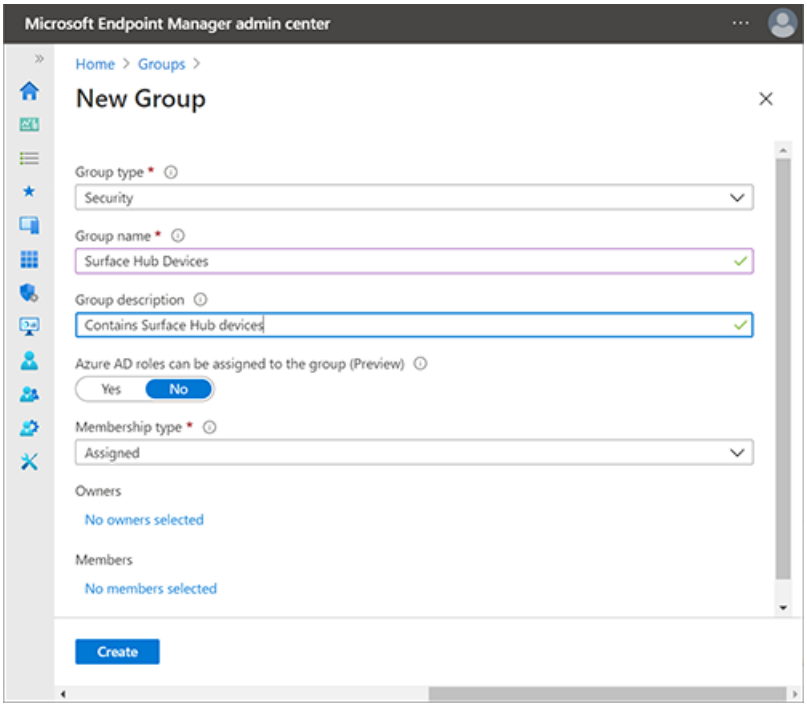
1. Inicie sesión en Intune a través Microsoft Endpoint Manager centrode administración, seleccione Grupos nuevos grupos > y, en Tipo de **** > **** grupo, seleccione **Seguridad.**
2. Escriba un nombre de grupo (por ejemplo, **Surface Hub administradores locales)** y, a continuación, **seleccione Crear.**



3. Abra el grupo, seleccione **Miembros**y, a continuación, elija Agregar miembros para especificar las cuentas de administrador que desea designar como administradores no globales en Surface Hub. **** Para obtener más información sobre cómo crear grupos en Intune, consulte Agregar grupos para organizar usuarios y dispositivos.

Crear grupo de seguridad para Surface Hub dispositivos

1. Repita el procedimiento anterior para crear un grupo de seguridad independiente para dispositivos concentradores; por ejemplo, **Surface Hub dispositivos**.



Obtener SID de grupo de Azure AD con PowerShell

1. Inicie PowerShell con privilegios de cuenta elevados (**Ejecutar**como administrador) y asegúrese de que el sistema está configurado para ejecutar scripts de PowerShell. Para obtener más información, consulte About Execution Policies.

2. Instalar Azure PowerShell módulo.

3. Inicie sesión en el inquilino de Azure AD.

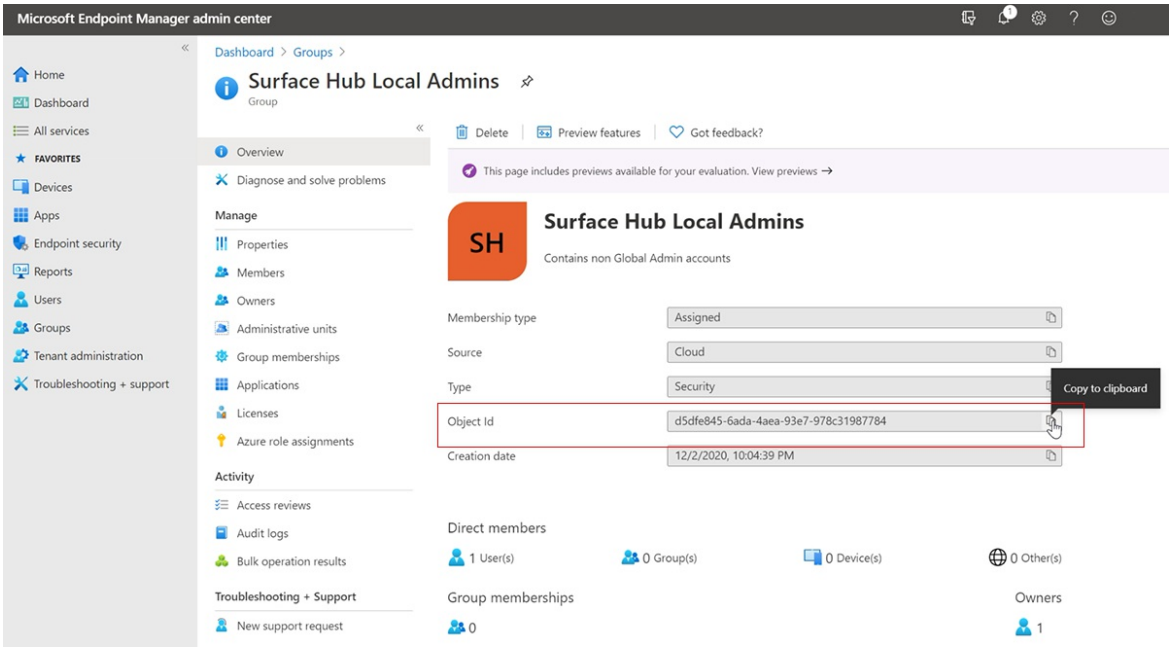
```
Connect-AzureAD
```

4. Cuando haya iniciado sesión en el inquilino, ejecute el siguiente commandlet. Se le pedirá que "Escriba el identificador de objeto de su grupo de Azure AD".

```
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. En Intune, seleccione el grupo que creó anteriormente y copie el identificador de objeto, como se muestra en la siguiente ilustración.



6. Ejecute el siguiente commandlet para obtener el SID del grupo de seguridad:

```
$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. Pegue el id. de objeto en el commandlet de PowerShell, presione **Entrar**y, a continuación, copie el **SID** de grupo de Azure AD en un editor de texto.

Crear archivo XML que contenga sid de grupo de Azure AD

1. Copie lo siguiente en un editor de texto:

```
<groupmembership>
<accessgroup desc = "S-1-5-32-544">
<member name = "Administrator" />
<member name = "S-1-12-1-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX" />
</accessgroup>
</groupmembership>
```

> **IMPORTANT**
>
> Es posible que deba usar el nombre localizado para la cuenta de administrador. No quite el miembro de administrador predeterminado del archivo XML.

2. Reemplace el SID de marcador de posición (empezando por S-1-12-1) por su **SID** de grupo de Azure AD y, a continuación, guarde el archivo como XML; por ejemplo, **aad-local-admin.xml**.

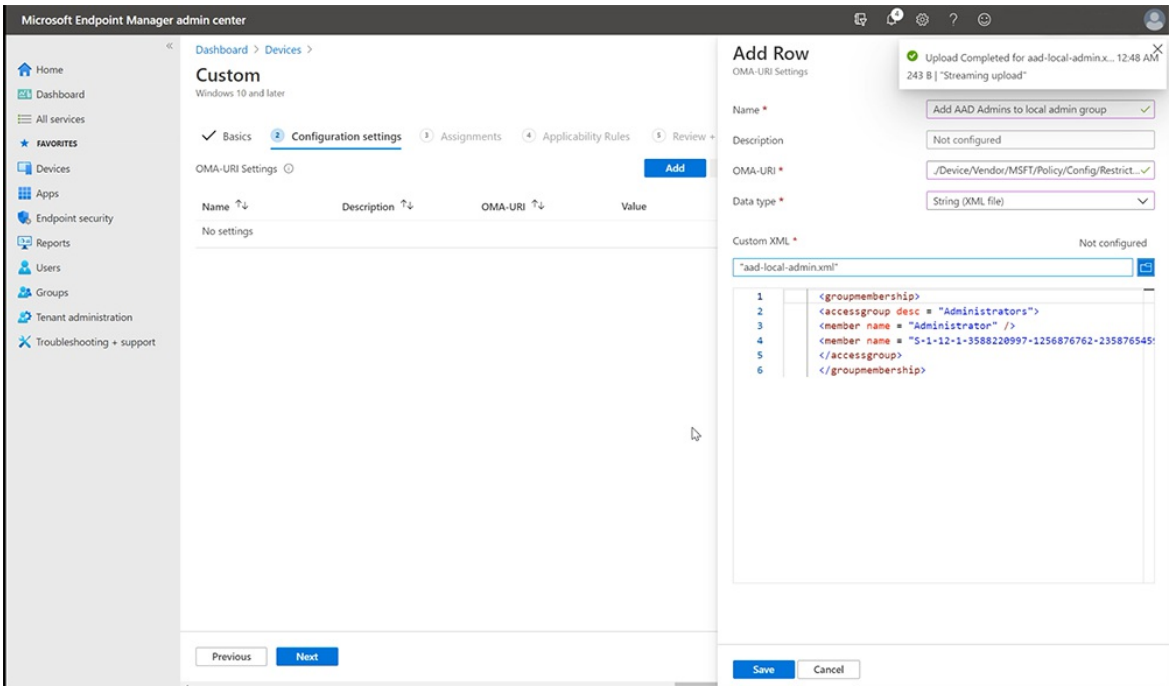
> **NOTE**
>
> Aunque los grupos deben especificarse a través de su SID, si desea agregar usuarios de Azure directamente, se pueden agregar especificando su nombre principal de usuario (UPN) en este formato:
> `<member name = "AzureAD\user@contoso.com" />`

Crear perfil de configuración personalizado

1. En Endpoint Manager, seleccione **Perfiles** > **de configuración de dispositivos Crear** > **perfil**.
2. En Plataforma, **seleccione Windows 10 y versiones posteriores.** En Perfil, seleccione **Personalizado**y, a continuación, **seleccione Crear.**
3. Agregue un nombre y una descripción y, a continuación, **seleccione Siguiente.**
4. En **Configuración** > **OMA-URI Configuración**, seleccione **Agregar**.
5. En el panel Agregar fila, agregue un nombre y, en **OMA-URI,** agregue la siguiente cadena:

```
./Device/Vendor/MSFT/Policy/Config/RestrictedGroups/ConfigureGroupMembership
```

6. En Tipo de datos, seleccione **String XML** y busque para abrir el archivo XML que creó en el paso anterior.



7. Haz clic en **Guardar**.
8. Haga **clic en Seleccionar grupos para incluir** y elegir el grupo de seguridad que creó anteriormente (Surface Hub**dispositivos**). Haz clic en **Siguiente**.
9. En Reglas de aplicabilidad, agregue una regla si lo desea. De lo contrario, **seleccione Siguiente** y, a continuación, **seleccione Crear**.

Para obtener más información sobre los perfiles de configuración personalizados con cadenas OMA-URI, vea Usar la configuración personalizada para Windows 10 dispositivos en Intune.

Administradores no globales que administran Surface Hub

Los miembros del **Surface Hub seguridad** de administradores locales ahora pueden iniciar sesión en la aplicación Configuración en Surface Hub y administrar la configuración.

> **IMPORTANT**
>
> Se quita el acceso predeterminado de los administradores globales a Configuración aplicación (a menos que también sean miembros de este nuevo grupo de seguridad).

Instalar aplicaciones en Microsoft Surface Hub

12/01/2022 • 7 minutes to read

Puedes instalar aplicaciones adicionales en tu Surface Hub para ajustarse a las necesidades de tu equipo u organización. Existen distintos métodos para instalar aplicaciones en función de si estás desarrollando y probando una aplicación o implementando una aplicación publicada. Este tema describe los métodos para instalar aplicaciones para cualquiera de esos escenarios.

Directrices de la aplicación admitidas

- Surface Hub solo puede ejecutar aplicaciones de la Plataforma universal de Windows (UWP). Las aplicaciones creadas con la herramienta de empaquetado MSIX no se ejecutarán en Surface Hub.
- Las aplicaciones deben elegirse para la familia de dispositivos universales o la familia de dispositivos del Equipo de Windows.
- Surface Hub solo admite aplicaciones con licencia sin conexión desde Microsoft Store para Empresas.
- De manera predeterminada, deben ser aplicaciones firmadas por la Store para poder instalarse. Durante la fase de desarrollo y prueba, también puedes elegir ejecutar aplicaciones para UWP firmadas por el desarrollador colocando el dispositivo en modo de desarrollador.
- Al enviar una aplicación al Microsoft Store, los desarrolladores deben establecer la disponibilidad de la familia de dispositivos y las opciones de licencias organizativas para asegurarse de que una aplicación estará disponible para ejecutarse en Surface Hub.
- Necesitas credenciales de administrador para instalar aplicaciones en el Surface Hub. Dado que el dispositivo está diseñado para usarse en espacios comunes como salas de reuniones, las personas no pueden acceder a la Microsoft Store para descargar e instalar aplicaciones.

Implementar aplicaciones publicadas

Hay varias opciones para la instalación de aplicaciones que se han publicado en la Microsoft Store en función de si quieres evaluarlas en algunos dispositivos o implementarlas ampliamente en tu organización.

Para instalar aplicaciones publicadas:

- Descarga la aplicación con la aplicación de la Microsoft Store, o
- Descarga el paquete de la aplicación de la Tienda Microsoft para Empresas y distribúyelo usando un paquete de aprovisionamiento o un proveedor de MDM compatible.

Aplicación de la Microsoft Store

Para evaluar aplicaciones publicadas de la Microsoft Store, usa la aplicación de la Microsoft Store en el Surface Hub para buscar y descargar aplicaciones.

> **NOTE**
> El uso de la aplicación de la Microsoft Store no es el método recomendado para implementar aplicaciones a escala en tu organización:
>
> - Para descargar aplicaciones, debes iniciar sesión en la aplicación de la Microsoft Store con una cuenta de Microsoft u organizativa. Sin embargo, solo puedes conectar una cuenta a un máximo de 10 dispositivos al mismo tiempo. Si tienes más de 10 Surface Hubs, deberás crear varias cuentas o quitar dispositivos de tu cuenta entre las instalaciones de las aplicaciones.
> - Para instalar aplicaciones, tendrás que iniciar sesión manualmente en la aplicación de la Microsoft Store en cada Surface Hub del que seas propietario.

Examinar la Microsoft Store en Surface Hub

1. En Surface Hub, inicia **Configuración**.
2. Escribe las credenciales de administrador del dispositivo cuando se solicite.
3. Vaya a **Surface Hub** > **aplicaciones & características**.
4. Selecciona **Abrir tienda** y busca la aplicación que estás buscando.

Descargar paquetes de la aplicación de la Tienda Microsoft para Empresas

Para descargar el paquete de la aplicación que necesitas para instalar aplicaciones en el Surface Hub, visita la Tienda Microsoft para Empresas. La Tienda para empresas es el lugar donde puedes buscar, comprar y administrar aplicaciones para los dispositivos Windows 10 de tu organización, incluido el Surface Hub.

> **NOTE**
> Actualmente, Surface Hub solo es compatible con aplicaciones con licencia sin conexión disponibles a través de la Tienda Microsoft para Empresas. Los desarrolladores de aplicaciones establecen la disponibilidad de la licencia sin conexión cuando envían las aplicaciones.

Busca y compra la aplicación que quieras y, a continuación, descarga:

- El paquete de la aplicación con licencia sin conexión (un .appx o un .appxbundle)
- El archivo de licencia *sin codificar* (si usas paquetes de aprovisionamiento para instalar la aplicación)
- La archivo de licencia *codificado* (si usas MDM para distribuir la aplicación)
- Los archivos de dependencia necesarios

Para obtener más información, consulta Descargar una aplicación con licencia sin conexión.

Instalar aplicaciones con licencia sin conexión a través del paquete de aprovisionamiento

Puedes instalar manualmente las aplicaciones con licencia sin conexión que hayas descargado de la Tienda para empresas en varios Surface Hubs mediante paquetes de aprovisionamiento. Usa Diseñador de imágenes y configuraciones de Windows (ICD) para crear un paquete de aprovisionamiento que contenga el paquete de la aplicación y el archivo de licencia *sin codificar* que descargaste de la Tienda para empresas. Para obtener más información, vea Create provisioning packages for Surface Hub.

Proveedor de MDM compatible

Para implementar aplicaciones en un gran número de Surface Hubs de tu organización, usa un proveedor de MDM compatible. La siguiente tabla muestra qué proveedores de MDM admiten la implementación de paquetes de aplicaciones con licencia sin conexión.

PROVEEDOR DE MDM	COMPATIBLE CON PAQUETES DE APLICACIONES CON LICENCIA SIN CONEXIÓN
MDM local con Configuration Manager (a partir de la versión 1602)	Sí
Proveedor de MDM de terceros	Comprueba que tu proveedor de MDM admite la implementación de paquetes de aplicaciones con licencia sin conexión.

NOTE

Para implementar aplicaciones sin conexión de forma remota mediante Microsoft Intune, consulte Manage VPP apps from Microsoft Store para Empresas. Surface Hub implementación de aplicaciones solo admite aplicaciones sin conexión que están asignadas a un grupo de dispositivos y usan el tipo de licencia Dispositivo.

Desarrollar y probar aplicaciones

En esta sección se proporciona información a los desarrolladores de aplicaciones para probar aplicaciones en Surface Hub.

Modo de desarrollador

De manera predeterminada, Surface Hub solo ejecuta aplicaciones para UWP que hayan sido publicadas y firmadas por la Microsoft Store. Las aplicaciones enviadas a la Microsoft Store se someten a pruebas de seguridad y cumplimiento como parte del proceso de certificación de la aplicación y esto permite proteger tu Surface Hub frente a aplicaciones malintencionadas.

Al habilitar el modo de desarrollador, también puedes instalar aplicaciones para UWP firmadas por el desarrollador.

IMPORTANT

Una vez habilitado el modo de desarrollador, deberás restablecer el Surface Hub para deshabilitarlo. Al restablecer el dispositivo se eliminan todas las configuraciones y los archivos de usuario locales y, a continuación, se vuelve a instalar Windows.

Activar el modo de desarrollador

1. En tu Surface Hub, inicia **Configuración**.
2. Escribe las credenciales de administrador del dispositivo cuando se solicite.
3. Navega hasta **Actualización y seguridad** > ** Para desarrolladores**.
4. Selecciona **Modo de desarrollador** y acepta la advertencia.

VisualStudio

Durante el desarrollo, la forma más sencilla de probar tu aplicación en un Surface Hub es usando Visual Studio. La característica de depuración remota de Visual Studio te ayuda a detectar problemas en tu aplicación antes de su implementación general. Para obtener más información, consulta Probar aplicaciones de Surface Hub con Visual Studio.

Crear paquete de aprovisionamiento

Usa Visual Studio para crear un paquete de la aplicación para tu aplicación para UWP, firmada mediante un certificado de prueba. A continuación, usa Diseñador de imágenes y configuraciones de Windows (ICD) para crear un paquete de aprovisionamiento que contenga el paquete de la aplicación. Para obtener más información,

vea Create provisioning packages for Surface Hub.

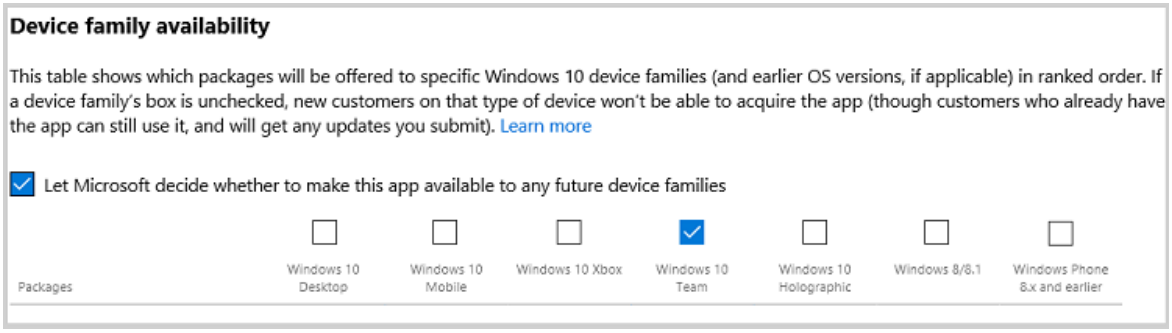
Enviar aplicaciones a la Microsoft Store

Cuando una aplicación está lista para publicarse, los desarrolladores necesitan enviarla y publicarla en la Microsoft Store. Para obtener más información, consulta Publicar Windows aplicaciones y juegos.

Durante el envío de la aplicación, los desarrolladores deben establecer la **disponibilidad de familias de dispositivos** y las opciones de **licencias de organización** para asegurarse de que la aplicación estará disponible para su ejecución en Surface Hub.

Establecer la disponibilidad de familias de dispositivos

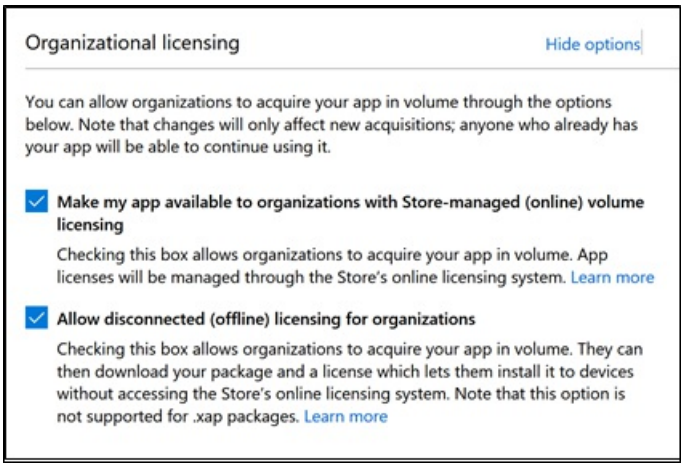
1. En el centro de desarrollo de Windows, ve a la página de envío de la aplicación.
2. Selecciona **Paquetes**.
3. En **Disponibilidad de familias de dispositivos**, selecciona estas opciones:
   - **Windows 10 Team**
   - **Permitir que Microsoft decida si quiere que la aplicación esté disponible para futuras familias de dispositivos**



Para obtener más información, consulta Disponibilidad de familias de dispositivos.

Establecer licencias de organización

1. En el centro de desarrollo de Windows, ve a la página de envío de la aplicación.
2. Selecciona **Precios y disponibilidad**.
3. En licencias de organización, selecciona **Permitir la compra de licencias en desconexión (sin conexión) para empresas**.



> **NOTE**
>
> **Hacer que mi aplicación esté disponible para organizaciones mediante la concesión de licencias administradas por Store (en línea) y distribución** está seleccionada de forma predeterminada.

> **NOTE**
>
> Los desarrolladores también pueden publicar aplicaciones de línea de negocio directamente en las empresas sin necesidad de que estén ampliamente disponibles en la Store. Para obtener más información, consulta Distribuir aplicaciones de LOB a empresas.

Para obtener más información, consulta Opciones de licencias de organización.

Resumen

Hay varias formas diferentes de instalar aplicaciones en tu Surface Hub según si estás desarrollando aplicaciones, evaluando aplicaciones en un número reducido de dispositivos o implementando aplicaciones de forma general en tu organización. En esta tabla se resumen los métodos admitidos:

MÉTODO DE INSTALACIÓN	DESARROLLO DE APLICACIONES	EVALUACIÓN DE APLICACIONES EN ALGUNOS DISPOSITIVOS	IMPLEMENTACIÓN DE APLICACIONES AMPLIAMENTE EN SU ORGANIZACIÓN
VisualStudio	X		
Paquete de aprovisionamiento	X	X	
Aplicación de la Microsoft Store		X	
Proveedor de MDM compatible			X

Administrar Microsoft Edge en Surface Hub

12/01/2022 • 3 minutes to read

Use Microsoft Edge de explorador para configurar la configuración del explorador Microsoft Edge a través de cualquiera de los siguientes métodos:

- Microsoft Intune
- El proveedor de administración de dispositivos móviles (MDM) preferido que admite la ingesta de ADMX
- Aprovisionar paquetes con admx ingestion en Windows Configuration Designer

> **TIP**
> El gesto de deslizar el dedo hacia abajo desde la parte superior de la pantalla para salir del modo de pantalla completa requiere dos dedos con el nuevo Microsoft Edge. La acción salir de pantalla completa también está disponible en el menú contextual que se muestra después de presionar durante mucho tiempo.

Directivas Microsoft Edge predeterminadas para Surface Hub

Microsoft Edge está preconfigurado con los siguientes conjuntos de directivas para proporcionar una experiencia optimizada para Surface Hub.

> **TIP**
> Se recomienda conservar el valor predeterminado para esta configuración de directiva.

CONFIGURACIÓN DE DIRECTIVA	EXPERIENCIA RECOMENDADA	VALOR PREDETERMINADO
AutoImportAtFirstRun	No importe automáticamente los tipos de datos y la configuración de Microsoft Edge (versión anterior). Esto evita cambiar los perfiles de los usuarios que han iniciado sesión con la configuración compartida de la Surface Hub.	4
BackgroundModeEnabled	Permitir Microsoft Edge los procesos para seguir ejecutándose en segundo plano incluso después de que se cierre la última ventana del explorador, lo que permite un acceso más rápido a las aplicaciones web durante una sesión.	1
BrowserAddProfileEnabled	No permitir que los usuarios creen nuevos perfiles en Microsoft Edge. Esto simplifica la experiencia de exploración y de sesión.	0

CONFIGURACIÓN DE DIRECTIVA	EXPERIENCIA RECOMENDADA	VALOR PREDETERMINADO
BrowserGuestModeEnabled	Permite que solo un usuario inicie sesión en Microsoft Edge. Esto simplifica la experiencia de exploración y de sesión	0
BrowserSignin	Permite a los usuarios disfrutar de single Sign-On (SSO) en Microsoft Edge. Cuando un usuario ha iniciado sesión Surface Hub, sus credenciales pueden fluir a los sitios web compatibles sin necesidad de que se vuelvan a autenticar.	1
ExtensionInstallBlockList	Impide que los usuarios que no son administradores instalen nuevas extensiones en Microsoft Edge. Para configurar una lista de extensiones que se instalarán de forma predeterminada, use ExtensionInstallForcelist.	*
HideFirstRunExperience	Oculta la primera experiencia de ejecución y la pantalla de presentación que normalmente se muestra cuando los usuarios ejecutan Microsoft Edge por primera vez. Dado Surface Hub es un dispositivo compartido, esto simplifica la experiencia del usuario.	1
InPrivateModeAvailability	Deshabilita el modo InPrivate. Dado que End Session ya borra los datos de exploración, esto simplifica la experiencia de exploración y de inicio de sesión.	1
NewTabPageSetFeedType	Muestra la Office 365 de fuentes en páginas de pestañas nuevas. Cuando un usuario ha iniciado sesión Surface Hub, esto permite un acceso rápido a sus archivos y contenido en Office 365.	1
NonRemovableProfileEnabled	Cuando un usuario ha iniciado sesión Surface Hub, se creará un perfil no extraíble con su cuenta organizativa. Esto simplifica la experiencia de single Sign-On (SSO).	1
PrintingEnabled	Deshabilita la impresión en Microsoft Edge. Surface Hub no admite la impresión.	0
ProActiveAuthEnabled	Permite Microsoft Edge autenticación proactiva de usuarios que han iniciado sesión con servicios Microsoft. Esto simplifica la experiencia de single Sign-On (SSO).	1

CONFIGURACIÓN DE DIRECTIVA	EXPERIENCIA RECOMENDADA	VALOR PREDETERMINADO
PromptForDownloadLocation	Guarda automáticamente los archivos en la carpeta Descargas, en lugar de preguntar a los usuarios dónde guardar el archivo. Esto simplifica la experiencia de exploración.	0

> **IMPORTANT**
> Actualmente, las aplicaciones web progresivas (PWA) no se admiten en el Windows 10 Team operativo. Tenga en cuenta también que Microsoft Edge configuración de directiva webAppInstallForceList no se admite en Surface Hub.

Configurar Microsoft Edge actualizaciones

De forma predeterminada, Microsoft Edge se actualiza automáticamente. Use Microsoft Edge de actualización para configurar la configuración de Microsoft Edge Update. Tenga en cuenta que Surface Hub no admite la configuración de directiva **CreateDesktopShortcut,** ya que Surface Hub no usa métodos abreviados de escritorio.

> **TIP**
> Microsoft Edge requiere conectividad a Internet para posibilitar sus funciones. Agregue las direcciones URL de dominio necesarias a la lista Permitir para garantizar las comunicaciones a través de firewalls y otros mecanismos de seguridad.

Vínculos relacionados

- Documentación de Microsoft Edge

Administrar Surface Hub con un proveedor MDM

12/01/2022 • 7 minutes to read

Surface Hub permite a los administradores de TI administrar la configuración y las directivas mediante un proveedor de administración de dispositivos móviles (MDM), como Microsoft Intune. Surface Hub tiene un componente de administración integrado para comunicarse con el servidor de administración. No es necesario instalar clientes adicionales en el dispositivo.

Inscripción de Surface Hub en la administración de MDM

Puedes inscribir Surface en Microsoft Intune otro proveedor mdm a través de la inscripción manual o automática.

Inscripción manual

1. Abre la **Configuración** e inicia sesión como administrador local. Seleccione **Surface Hub** > **Administración de dispositivos** y, a continuación, seleccione **+Administración de dispositivos**.
2. Se te pedirá que inicies sesión con la cuenta que usarás para tu proveedor mdm. Después de autenticar, el dispositivo se inscribe automáticamente con el proveedor mdm.

> **TIP**
> Si usa Intune y no se detecta la dirección del servidor, escriba **manage.microsoft.com**.

> **NOTE**
> La inscripción de MDM usa los detalles de la cuenta proporcionados para la autenticación. La cuenta debe tener permisos para inscribir un dispositivo Windows, así como una licencia de Intune (o las licencias de inscripción equivalentes configuradas en el proveedor MDM de terceros).

Inscripción automática: afiliada a Azure AD

Durante el proceso de configuración inicial, al asociar Surface Hub con un inquilino de Azure Active Directory (AD) que tenga habilitada la inscripción automática de Intune, el dispositivo se inscribirá automáticamente en Intune. Para obtener más información, consulte Intune enrollment methods for Windows devices. La afiliación de Azure AD y la inscripción automática de Intune son necesarias para que Surface Hub sea un "dispositivo compatible" en Intune.

Administrar Surface Hub Windows 10 Team configuración con Intune

El bloque de creación fundamental de la administración de la configuración de directivas en Intune y otros proveedores de MDM es el protocolo open mobile Alliance-Device management (OMA-DM) basado en XML. Windows 10 implementa OMA-DM XML a través de uno de los muchos proveedores de servicios de configuración (CSP) disponibles con nombres como AccountManagement CSP, DeviceStatus CSP, WiFi-CSP, entre otros. Para obtener una lista completa, consulte LOSP compatibles con Microsoft Surface Hub.

Microsoft Intune y otros proveedores de MDM usan CSP para ofrecer una interfaz de usuario que te permita configurar las opciones de directiva en los perfiles de configuración. Intune usa el CSP de Surface Hub para su perfil integrado (restricciones de **dispositivos (Windows 10 Team),** lo que te permite configurar opciones básicas como impedir que Surface Hub "se desenlome" cada vez que alguien se mueva cerca dentro de su intervalo de proximidad. Para administrar la configuración del concentrador y las características fuera del perfil

integrado de Intune, deberá usar un perfil personalizado, como se muestra a continuación.

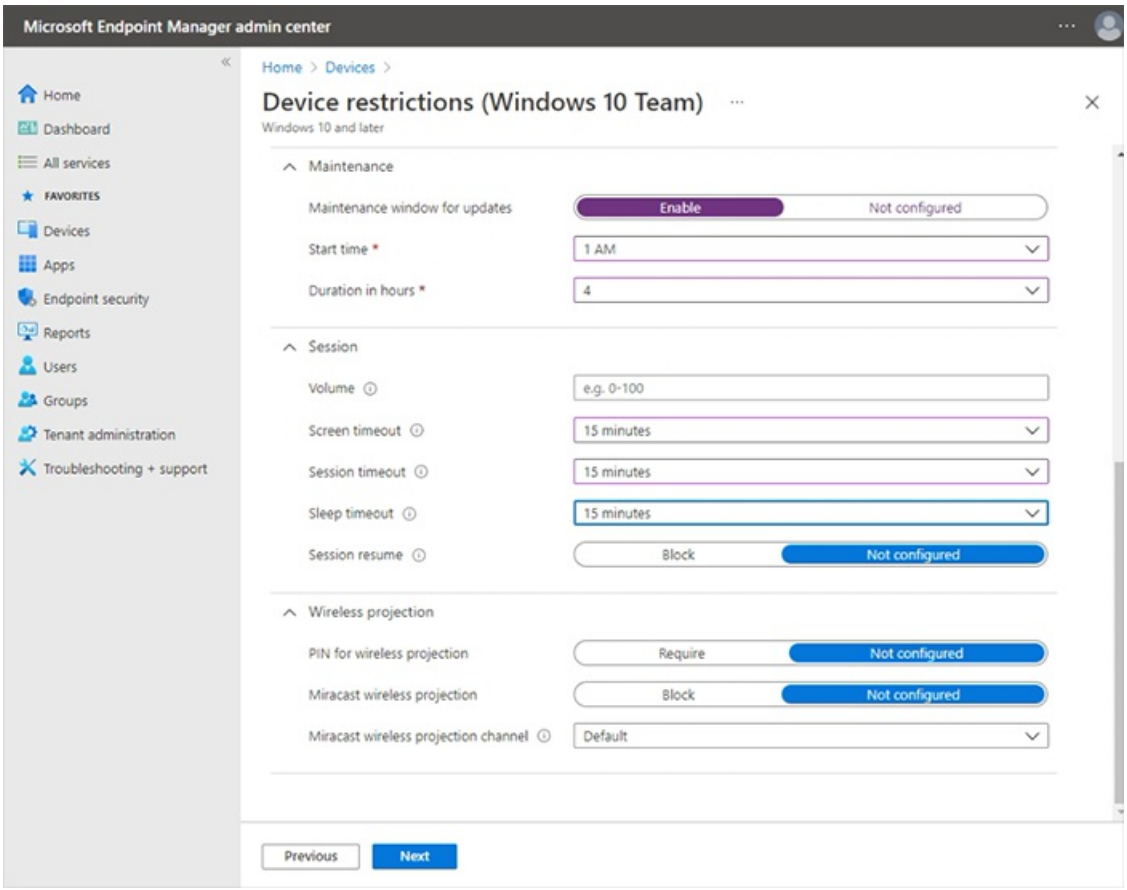
En resumen, las opciones para configurar y administrar la configuración de directivas en Intune incluyen lo siguiente:

- **Crear un perfil de restricción de dispositivo.** Usa el perfil integrado de Intune y configura la configuración directamente en la interfaz de usuario de Intune. Consulta Crear perfil de restricción de dispositivos.
- **Crear un perfil de configuración de dispositivo.** Seleccione una plantilla centrada en una característica o tecnología específica, como Microsoft Defender o certificados de seguridad. Consulta Crear perfil de configuración de dispositivo.
- **Crear un perfil de configuración personalizado.** Amplíe el ámbito de administración mediante un identificador uniforme de recursos (URI de OMA) de OMA desde cualquiera de los CSP admitidos en Microsoft Surface Hub. Consulte Crear perfil de configuración personalizado.

> **NOTE**
> Los perfiles deben asignarse a grupos de dispositivos que contengan los dispositivos Surface Hub inscritos.

Crear perfil de restricción de dispositivos

1. Inicie sesión en el **Microsoft Endpoint Manager de administración**, seleccione **** > **Perfiles de configuración de dispositivos** > **+ Crear perfil**.
2. En **Plataforma**, **seleccione Windows 10 y versiones posteriores** >
3. En ****Tipo de**perfil,** seleccione **Plantillas** y, a continuación, **seleccione Restricciones de dispositivo (Windows 10 Team)**
4. Seleccione **Crear**, agregar un nombre y, a continuación, **seleccione Siguiente.**
5. Ahora puede examinar y elegir entre la configuración de restricción de dispositivos preestablecida para Surface Hub en las siguientes categorías: Aplicaciones y experiencia, Información operativa de Azure, Mantenimiento, Sesión y proyección inalámbrica. En el ejemplo que se muestra en la figura siguiente se especifica una ventana de mantenimiento de 4 horas y un tiempo de espera de 15 minutos para la pantalla, el suspensión y la reanudación de la sesión.



Para obtener más información acerca de la creación y administración de perfiles, vea Restringir las características de dispositivosmediante la directiva en Microsoft Intune .

Para obtener más información acerca de cómo administrar las Surface Hub y la configuración, consulta Surface Hub Windows 10 Team restricciones de dispositivos en Microsoft Intune

Crear perfil de configuración de dispositivo

1. Inicie sesión en el **Microsoft Endpoint Manager de administración,**seleccione **Perfiles** > **de configuración de dispositivos** > **+ Crear perfil**.
2. En **Plataforma**, **seleccione Windows 10 y versiones posteriores** >
3. En **Tipo de perfil,** seleccione **Plantillas** y elija entre las siguientes plantillas admitidas en Surface Hub:
   - Restricciones de dispositivos (Windows 10 Team), como se describe en la sección anterior.
   - Microsoft Defender para endpoint (Windows 10 Desktop)
   - Certificado PKCS
   - Certificado importado de PKCS
   - Certificado SCEP
   - Certificado de confianza

Crear perfil de configuración personalizado

Puede ampliar el ámbito de administración mediante la creación de un perfil personalizado mediante un URI de OMA desde cualquiera de los CSP admitidosen Microsoft Surface Hub . Cada configuración de un CSP tiene un OMA-URI correspondiente que puede establecer mediante perfiles de configuración personalizados en Intune. Para obtener información detallada sobre los SURFACE HUB, puede hacer referencia a los siguientes recursos:

- Referencia de proveedor de servicios de configuración
- CSP de directivas admitidas por Microsoft Surface Hub

- SurfaceHub CSP

> **NOTE**
> La administración de la cuenta del dispositivo mediante la configuración del CSP de SurfaceHub no es posible actualmente con Intune y requiere el uso de un proveedor MDM de terceros.

Para implementar la configuración de directiva basada en CSP, empiece generando un URI de OMA y, a continuación, agrégrelo a un perfil de configuración personalizado en Intune.

Generar URI de OMA para la configuración de destino

Para generar el URI de OMA para cualquier configuración:

1. En la documentación de CSP,identifique el nodo raíz del CSP. Por lo general, esto tiene el aspecto **./Vendor/MSFT/NameOfCSP**.
   - **Ejemplo:** El nodo raíz del CSP de SurfaceHub es **./Vendor/MSFT/SurfaceHub**.
2. Identificar la ruta de acceso del nodo para la configuración que quieras usar.
   - **Ejemplo:** La ruta de acceso de nodo para la configuración para habilitar la proyección inalámbrica es **InBoxApps/WirelessProjection/Enabled**.
3. Anexar la ruta de acceso del nodo raíz para generar el URI de OMA.
   - **Ejemplo:** El URI de OMA para la configuración para habilitar la proyección inalámbrica es **./Vendor/MSFT/SurfaceHub/InBoxApps/WirelessProjection/Enabled.**
4. El tipo de datos también se indica en la documentación de CSP. Los tipos de datos más comunes son:
   - char (Cadena)
   - int (Entero)
   - bool (Booleano)

Agregar URI de OMA al perfil de configuración personalizado

1. En Endpoint Manager, seleccione **Perfiles** > **de configuración de dispositivos Crear** > **perfil**.
2. En Plataforma, **seleccione Windows 10 y versiones posteriores.** En Perfil, seleccione **Personalizado**y, a continuación, **seleccione Crear.**
3. Agregue un nombre y una descripción opcional y, a continuación, **seleccione Siguiente.**
4. En **Configuración** > **OMA-URI Configuración**, seleccione **Agregar**.

Microsoft Teams y Skype Empresarial configuración

En esta sección se Teams y Skype Empresarial que puedes administrar a través de Intune u otro proveedor MDM. Esto incluye:

- Calidad del servicio (QoS)
- Administrar Teams características específicas del usuario

Configuración de calidad del servicio

Para garantizar una calidad óptima de vídeo y audio en Surface Hub, agrega la siguiente configuración de QoS al dispositivo.

NOMBRE	DESCRIPCIÓN	OMA-URI	TIPO	VALOR
Puertos de audio	Rango de puertos de audio	./Device/Vendor/MSFT/NetworkQoSPolicy/Audio/SourcePortMatchCondition	Cadena	50000-50019

NOMBRE	DESCRIPCIÓN	OMA-URI	TIPO	VALOR
DSCP de audio	Marcado de puertos de audio	./Device/Vendor/MSFT/NetworkQoSPolicy/Audio/DSCPAction	Integer	46
Puertos de vídeo	Rango de puertos de vídeo	./Device/Vendor/MSFT/NetworkQoSPolicy/Video/SourcePortMatchCondition	Cadena	50020-50039
DSCP de vídeo	Marcado de puertos de vídeo	./Device/Vendor/MSFT/NetworkQoSPolicy/Video/DSCPAction	Integer	34
Puertos de uso compartido	Intervalo de puertos compartidos	./Device/Vendor/MSFT/NetworkQoSPolicy/Sharing/SourcePortMatchCondition	Cadena	50040-50059
Uso compartido de DSCP	Marcado de puertos compartidos	./Device/Vendor/MSFT/NetworkQoSPolicy/Sharing/DSCPAction	Integer	18

> **NOTE**
> En la tabla se muestran los intervalos de puertos predeterminados. Los administradores pueden cambiar los intervalos de puertos en Skype Empresarial y en el panel de control de Teams.

Administrar Teams características específicas del usuario

Puede crear un perfil de configuración personalizado para administrar Teams reuniones coordinadas, la unión de proximidad y otras características. Para obtener más información, vea Manage Microsoft Teams configuration on Surface Hub.

Cambiar la aplicación predeterminada para las reuniones & llamadas

La aplicación predeterminada para reuniones & llamadas en el Surface Hub varía en función de cómo instales Windows 10 Team 2020 Update (también Windows 10 20H2 Team edition). Si vuelves a crear una imagen Surface Hub a Windows 10 20H2, Microsoft Teams se establecerá como el valor predeterminado, sin que Skype Empresarial esté disponible (modo 1). Si actualiza el concentrador desde una versión anterior del sistema operativo, Skype Empresarial permanecerá como predeterminado, con la funcionalidad Teams disponible (modo 0) a menos que ya haya configurado Teams como predeterminado.

Para cambiar la instalación predeterminada, use un perfil personalizado para establecer el Teams de reunión de la siguiente manera:

- Modo 0: Skype Empresarial con la funcionalidad de Microsoft Teams para reuniones programadas.
- Modo 1: Microsoft Teams solo.

NOMBRE	DESCRIPCIÓN	OMA-URI	TIPO	VALOR
Id. de aplicación de Teams	Nombre de la aplicación	./Vendor/MSFT/SurfaceHub/Properties/VtcAppPackageId	Cadena	Microsoft.MicrosoftTeamsforSurfaceHub_8wekyb3d8bbwe!Teams

NOMBRE	DESCRIPCIÓN	OMA-URI	TIPO	VALOR
Modo de aplicación de Teams	Modo Teams	./Vendor/MSFT/SurfaceHub/Properties/SurfaceHubMeetingMode	Integer	0 o 1

Configurar el menú Inicio de Surface Hub

12/01/2022 • 3 minutes to read

La actualización de 17 de enero de 2018 a Windows 10 (compilación 15063.877) permite menús Inicio personalizados en dispositivos Surface Hub. Aplica el diseño del menú Inicio personalizado usando administración de dispositivos móviles (MDM).

Al aplicar un diseño de menú Inicio personalizado a Surface Hub, los usuarios no pueden anclar, desanclar ni desinstalar aplicaciones desde Inicio.

Cómo aplicar un menú Inicio personalizado a Surface Hub

El menú Inicio personalizado se define en un archivo XML de diseño de Inicio. Tienes dos opciones para crear el archivo XML de diseño de Inicio:

- Editar el XML de Inicio de Surface Hub predeterminado

  O bien

- Configurar el menú Inicio deseado en un equipo de escritorio (anclando solo aplicaciones que estén disponibles en Surface Hub) y luego exportar el diseño.

> **TIP**
> Para agregar una ventana con un vínculo web al menú Inicio de escritorio, ve al vínculo en Microsoft Edge, selecciona `...` en la esquina superior derecha y selecciona **Anclar esta página a Inicio**. Consulta un diseño de Inicio que incluya un vínculo de Microsoft Edge para ver un ejemplo de cómo aparecerán los vínculos en el XML.

Para editar el XML predeterminado o el diseño exportado, familiarízate con el XML de diseño de Inicio. Hay unas pocas diferencias entre el diseño de Inicio en un escritorio y en Surface Hub.

Cuando tengas el menú Inicio definido en un XML de diseño de Inicio, crea una directiva MDM para aplicar el diseño.

Diferencias entre los menús Inicio de Surface Hub y de escritorio

Existen unas pocas diferencias clave entre la personalización del menú Inicio para Surface Hub y para un escritorio de Windows 10:

- No puede usar **DesktopApplicationTile en** el XML de diseño de inicio porque Windows aplicaciones de escritorio (Win32) no se admiten en Surface Hub.
- No puedes usar el XML de diseño de Inicio para configurar la barra de tareas o la pantalla de inicio de sesión de Surface Hub.
- La directiva de diseño de inicio solo debe asignarse a dispositivos, no a usuarios.
- La configuración de OMA-URI que se va a usar en la directiva es `./Device/Vendor/MSFT/Policy/Config/Start/StartLayout`
- Surface Hub admite un máximo de 6 columnas (6 ventanas 1 x 1); sin embargo, **debes** definir `GroupCellWidth=8` incluso aunque Surface Hub muestre solo ventanas de pantalla en las columnas 0 - 5, y no en las columnas 6 y 7.
- Surface Hub admite un número máximo de 6 filas (6 iconos de 1 x 1)

- `SecondaryTile`, que se usa para vínculos, que abrirán el vínculo en Microsoft Edge.

Ejemplo: Diseño de Inicio de Surface Hub predeterminado

```
<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/FullDefaultLayout">
        <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>
```

Ejemplo: Diseño de Inicio que incluye un vínculo de Microsoft Edge

Este ejemplo muestra un vínculo a un sitio web y un vínculo a un archivo .pdf. El icono secundario de Microsoft Edge usa un icono de 150 x 150 píxeles.

```
<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/FullDefaultLayout">
        <start:Group Name="" xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout">
    <start:Tile
              AppUserModelID="Microsoft.Office.PowerPoint_8wekyb3d8bbwe!Microsoft.pptim"
              Size="2x2"
              Row="0"
              Column="0"/>
          <start:Tile
              AppUserModelID="Microsoft.Office.Word_8wekyb3d8bbwe!Microsoft.Word"
              Size="2x2"
              Row="0"
              Column="2"/>
          <start:Tile
              AppUserModelID="Microsoft.Office.Excel_8wekyb3d8bbwe!Microsoft.Excel"
              Size="2x2"
              Row="0"
              Column="4"/>
          <start:DesktopApplicationTile
              DesktopApplicationID="MSEdge"
              Size="2x2"
              Row="2"
              Column="0"/>
    <start:Tile
              AppUserModelID="microsoft.microsoftskydrive_8wekyb3d8bbwe!App"
              Size="2x2"
             Row="2"
             Column="2"/>
  <start:SecondaryTile
            AppUserModelID="Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge"
           TileID="2678823080"
           DisplayName="Bing"
           Arguments="https://www.bing.com/"
           Square150x150LogoUri="ms-appx:///"
           Wide310x150LogoUri="ms-appx:///"
           ShowNameOnSquare150x150Logo="true"
           ShowNameOnWide310x150Logo="false"
           BackgroundColor="#ffe9e7e7"
           ForegroundText="dark"
           Size="2x2"
           Column="4"
           Row="2"  />
    <start:Tile
              AppUserModelID="Microsoft.Windows.Photos_8wekyb3d8bbwe!App"
              Size="2x2"
              Row="4"
              Column="0"/>
    <start:SecondaryTile
             AppUserModelID="Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge"
             TileID="6153963000"
             DisplayName="cstrtqbiology.pdf"
             Arguments="-contentTile -formatVersion 0x00000003 -pinnedTimeLow 0x45b7376e -pinnedTimeHigh
0x01d2356c -securityFlags 0x00000000 -tileType 0x00000000 -url 0x0000003a
https://www.ada.gov/regs2010/2010ADAStandards/Guidance_2010ADAStandards.pdf"
             Square150x150LogoUri="ms-appx:///Assets/MicrosoftEdgeSquare150x150.png"
             Wide310x150LogoUri="ms-appx:///"
             ShowNameOnSquare150x150Logo="true"
             ShowNameOnWide310x150Logo="false"
             BackgroundColor="#ff4e4248"
             Size="4x2"
             Row="4"
             Column="2"/>
        </start:Group>
      </defaultlayout:StartLayout>
```

```
    </StartLayoutCollection>
  </DefaultLayoutOverride>
</LayoutModificationTemplate>
```

> **NOTE**
>
> El valor predeterminado de es light; no es necesario incluirlo en el XML a menos que cambie el `ForegroundText` `ForegroundText` valor a oscuro.

Administración local para la configuración de Surface Hub

12/01/2022 • 4 minutes to read

Tras la configuración inicial de Microsoft Surface Hub, la configuración del dispositivo se puede administrar localmente mediante **Configuración**.

Configuración de Surface Hub

Los Surface Hubs tienen muchas opciones que son comunes a otros dispositivos Windows, pero también tienen opciones de configuración que solo se pueden configurar en los Surface Hubs. En esta tabla se enumeran las opciones de configuración que solo son configurables en los Surface Hubs.

VALOR	UBICACIÓN	DESCRIPCIÓN
Cuenta del dispositivo	Surface Hub > Cuentas	Establecer o cambiar la cuenta del dispositivo de Surface Hub.
Estado de sincronización de la cuenta del dispositivo	Surface Hub > Cuentas	Comprobar el estado de la sincronización del correo electrónico y el calendario de la cuenta del dispositivo en Surface Hub.
Rotación de contraseñas	Surface Hub > Cuentas	Elegir si se permite que el Surface Hub rote automáticamente la contraseña de la cuenta del dispositivo.
Cambiar la contraseña de la cuenta de administrador	Surface Hub > Cuentas	Cambiar la contraseña de la cuenta de administrador local. Esta característica solo está disponible si has configurado el dispositivo para usar un administrador local durante la primera ejecución.
Administración del dispositivo	Surface Hub > Administración de dispositivos	Administrar las directivas y aplicaciones empresariales mediante la administración de dispositivos móviles (MDM).
Paquetes de aprovisionamiento	Surface Hub > Administración de dispositivos	Establecer o cambiar los paquetes de aprovisionamiento instalados en el Surface Hub.
Abrir la aplicación Microsoft Store	Surface Hub > Aplicaciones y características	La aplicación Microsoft Store solo está disponible para los administradores a través de la aplicación Configuración.
Nombre de dominio de Skype Empresarial	Surface Hub > Llamadas y audio	Configurar un nombre de dominio de tu Skype Empresarial Server.

VALOR	UBICACIÓN	DESCRIPCIÓN
Volumen de altavoz predeterminado	Surface Hub > Llamadas y audio	Configurar el volumen del altavoz predeterminado para el Surface Hub cuando se inicia una sesión.
Configuración predeterminada de micrófono y altavoces	Surface Hub > Llamadas y audio	Configurar un micrófono y un altavoz predeterminados para las llamadas y un altavoz predeterminado para la reproducción de contenido multimedia.
Habilitar Dolby Audio X2	Surface Hub > Llamadas y audio	Configurar las mejoras de altavoces Dolby Audio X2.
Abrir la aplicación Conectar automáticamente	Surface Hub > Proyección	Elegir si la proyección abrirá automáticamente la aplicación Conectar o si debe esperar a la entrada del usuario antes de abrirla.
Desactivar la proyección inalámbrica con Miracast	Surface Hub > Proyección	Elegir si los moderadores pueden proyectar de forma inalámbrica en Surface Hub con Miracast.
Requerir un PIN para la proyección inalámbrica	Surface Hub > Proyección	Elegir si los contactos tienen que escribir un PIN antes de usar la proyección inalámbrica.
Canal de proyección inalámbrica (Miracast)	Surface Hub > Proyección	Establecer el canal para la proyección de Miracast.
Información de la reunión que se muestra en la pantalla de inicio de sesión	Surface Hub > Pantalla de inicio de sesión	Elegir si el organizador de la reunión, la hora y el asunto se mostrarán en la pantalla de inicio de sesión.
Fondo de pantalla de inicio de sesión	Surface Hub > Pantalla de inicio de sesión	Elija una imagen que se usará como fondo durante las sesiones de usuario y en la pantalla de bienvenida.
Tiempo de espera de sesión a la pantalla de bienvenida	Surface Hub > de & sesión	Elegir cuánto tiempo hasta que Surface Hub vuelve a la pantalla de inicio después de que no se detecte ningún movimiento.
Reanudar la sesión	Surface Hub > de & sesión	Elegir si se debe permitir que los usuarios reanuden la sesión después de que no se detecté ningún movimiento o limpiar automáticamente una sesión.
Acceso a archivos y reuniones de Office 365	Surface Hub > de & sesión	Elige si un usuario puede iniciar sesión en Office 365 para acceder a sus reuniones y archivos.
Activar la pantalla con sensores de movimiento	Surface Hub > de & sesión	Elegir si la pantalla se activa cuando se detecte movimiento.

VALOR	UBICACIÓN	DESCRIPCIÓN
Tiempo de espera de pantalla	Surface Hub > de & sesión	Elige cuánto tiempo debe estar inactivo el dispositivo antes de desactivar la pantalla.
Tiempo de espera de suspensión	Surface Hub > de & sesión	Elegir cuánto tiempo el dispositivo debe estar inactivo antes de pasar al modo de suspensión.
Nombre descriptivo	Surface Hub > Acerca de	Establecer el nombre del Surface Hub que los contactos verán al conectarse de forma inalámbrica.
Horas de mantenimiento	Actualización y seguridad > Windows Update > Opciones avanzadas	Configurar cuando se pueden instalar actualizaciones.
Recuperar desde la nube	Actualización y seguridad > Recuperación	Reinstalar el sistema operativo en Surface Hub a una compilación del fabricante desde la nube.
Guardar la clave de BitLocker	Actualización y seguridad > Recuperación	Hacer copia de seguridad de la clave de BitLocker de tu Surface Hub en una unidad USB.
Recopilar registros	Actualización y seguridad > Recuperación	Guardar los registros en una unidad USB para enviar a Microsoft más adelante.

Temas relacionados

Administrar la configuración de Surface Hub

Administración remota de Surface Hub

Guía del administrador de Microsoft Surface Hub

Administración de contraseñas (Surface Hub)

12/01/2022 • 2 minutes to read

Cada cuenta del dispositivo de Microsoft Surface Hub requiere una contraseña para autenticarse y habilitar características en el dispositivo. Por motivos de seguridad, es posible que quieras cambiar (o "rotar") esta contraseña con regularidad. Sin embargo, si la contraseña de la cuenta del dispositivo cambia, la contraseña que estaba almacenada en el dispositivo Surface Hub no será válida y se deshabilitarán todas las características que dependan de dicha cuenta del dispositivo. Tendrás que actualizar la contraseña de la cuenta del dispositivo en el Surface Hub desde la aplicación Configuración para volver a habilitar estas características.

Para simplificar la administración de contraseñas de las cuentas de dispositivo de Surface Hub, hay dos opciones:

1. Desactivar la expiración de la contraseña para la cuenta del dispositivo.
2. Permitir que el dispositivo Surface Hub rote automáticamente la contraseña de la cuenta del dispositivo.

Desactivar la rotación de contraseñas para la cuenta del dispositivo.

Establece la propiedad **PasswordNeverExpires** de la cuenta del dispositivo en True. Deberías comprobar si se cumplen los requisitos de seguridad de la organización.

Permitir que el Surface Hub rote automáticamente la contraseña de la cuenta del dispositivo

El Surface Hub puede cambiar automáticamente la contraseña de una cuenta de dispositivo sin necesidad de actualizarla manualmente. Puede habilitar esta característica en **Configuración** > **Surface Hub** > **Cuentas**. Si activa la rotación de contraseñas, Surface Hub intentará cambiar la contraseña cada 7 días durante el horario de mantenimiento. Las contraseñas no cambian durante una reunión. Si han transcurrido 7 días desde la última rotación de contraseña, pero el Surface Hub estaba desactivado, intentará cambiar la contraseña inmediatamente cuando se haya activado o cada 10 minutos hasta que se haya realizado correctamente.

Las contraseñas generadas automáticamente contienen de 15 a 32 caracteres, incluida una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Ten en cuenta que cuando se cambie la contraseña de la cuenta del dispositivo, no se mostrará la nueva contraseña. Si necesitas iniciar sesión en la cuenta o volver a proporcionar la contraseña (por ejemplo, si quieres cambiar la configuración de la cuenta de dispositivo en el Surface Hub), necesitarás usar Active Directory o el portal de administración de Microsoft 365 para restablecer la contraseña.

> **IMPORTANT**
>
> La opción de afiliación de dispositivos seleccionada durante la configuración inicial del Surface Hub tiene un impacto en el formato de cuenta del dispositivo que se puede usar con el giro de contraseña. Los concentradores asociados con un Active Directory local solo pueden girar las contraseñas de las cuentas de dispositivo especificadas en **formato dominio\nombredeusuario**. Los concentradores asociados con un Azure Active Directory solo pueden girar las contraseñas de las cuentas de dispositivo especificadas en formato, pero solo si la cuenta es solo en la nube o si el dominio de AAD está configurado para la autenticación en la nube y la escritura de escritura de `username@domain.com` contraseñas.

Administrar actualizaciones de Windows en Surface Hub

12/01/2022 • 7 minutes to read

Las nuevas versiones del sistema operativo de Surface Hub se publican a través de Windows Update, igual que las versiones de Windows 10. Esta página explica los procedimientos recomendados para administrar actualizaciones de dispositivos Surface Hub.

Windows Update para empresas

Windows Update para empresas es un conjunto de características diseñadas para proporcionar a las empresas un control adicional sobre cómo y cuándo instala Windows Update las versiones, a la vez que reduce los costos de administración de dispositivos. Con este método, los Surface Hubs están conectados directamente al servicio Windows Update de Microsoft.

- Recibir actualizaciones directamente del servicio Windows Update de Microsoft, sin ninguna infraestructura adicional necesaria.
- Aplazar actualizaciones para proporcionar más tiempo para pruebas y evaluaciones.
- Implementar actualizaciones para seleccionar grupos de dispositivos.
- Definir ventanas de mantenimiento para instalar actualizaciones.

> **TIP**
> Usar el uso compartido de contenido de punto a punto para reducir los problemas de ancho de banda durante las actualizaciones. Consulta Optimizar la distribución de actualizaciones de Windows10 para obtener más información.

> **NOTE**
> Surface Hub no admite actualmente revertir las actualizaciones.

Modelo de mantenimiento de Surface Hub

Surface Hub usa el modelo de mantenimiento de Windows 10, que se denomina Windows como servicio (WaaS). Tradicionalmente, las nuevas características se agregan solo en las nuevas versiones de Windows que se publican cada pocos años. Cada nueva versión requiere implementar procesos largos y costosos en una organización. Como resultado, los usuarios finales y las organizaciones no suelen disfrutar de las ventajas de las nuevas innovaciones. El objetivo de Windows como servicio es proporcionar continuamente nuevas funcionalidades y mantener al mismo tiempo un alto nivel de calidad.

Microsoft publica dos tipos de versiones de Surface Hub ampliamente de manera continua:

- **Actualizaciones de características** - Actualizaciones que instalan las funciones, experiencias y capacidades nuevas más recientes. Microsoft espera publicar dos nuevas actualizaciones de características por año.
- **Actualizaciones de calidad** - Actualizaciones que se centran en la instalación de revisiones de seguridad, controladores y otras actualizaciones de mantenimiento. Microsoft espera publicar una actualización de calidad acumulativa cada mes.

A fin de mejorar la calidad de las versiones y simplificar las implementaciones, todas las nuevas versiones que Microsoft publique para Windows 10, incluidas las de Surface Hub, serán acumulativas. Esto significa que las nuevas actualizaciones de características y de calidad incluirán las cargas de todas las versiones anteriores (de forma optimizada para reducir los requisitos de almacenamiento y de redes) y la instalación de la versión en un dispositivo hará que este esté totalmente actualizado. Además, a diferencia de las versiones anteriores de Windows, no puedes instalar un subconjunto del contenido de una actualización de calidad de Windows 10. Por ejemplo, si una actualización de calidad incluye correcciones para tres vulnerabilidades de seguridad y un problema de confiabilidad, la implementación de la actualización dará como resultado la instalación de las cuatro correcciones.

El sistema operativo de Surface Hub recibe actualizaciones en el Canal semianual. Al igual que otras ediciones de Windows 10, el período de duración de mantenimiento es finito. Debes instalar actualizaciones de nuevas características en equipos que ejecuten estas ramas para seguir recibiendo actualizaciones de calidad.

Para obtener más información acerca de Windows como servicio, consulta Información general de Windows como servicio.

Usar Windows Update para empresas

Surface Hubs, como todos los dispositivos Windows 10, incluye **Windows Update para empresas (WUfB)** que te permite controlar cómo se actualizan los dispositivos. Windows Update para empresas ayuda a reducir los costos de administración de dispositivos y ofrece el control sobre la implementación de actualizaciones, así como acceso rápido a actualizaciones de seguridad y a las últimas innovaciones de Microsoft de manera continua. Para obtener más información, consulta Administrar actualizaciones con Windows Update para empresas.

Para configurar Windows Update para empresas:

1. Agrupar Surface Hub en anillos de implementación
2. Configurar cuándo recibe actualizaciones Surface Hub.

> **NOTE**
> Puede usar Microsoft Intune, Microsoft Endpoint Configuration Manager o un proveedor de MDM de terceros compatible para configurar WUfB. Tutorial: usar Microsoft InTune para configurar Windows Update para empresas.

Agrupar Surface Hub en anillos de implementación

Usa anillos de implementación para controlar cuándo se lanzan las actualizaciones para tus Surface Hubs, dándote tiempo para que las valides. Por ejemplo, puedes actualizar un grupo reducido de dispositivos para comprobar la calidad antes de realizar un lanzamiento general en tu organización. En función de quién administre Surface Hub en tu organización, considera la posibilidad de incorporar Surface Hub en los anillos de implementación generados para tus otros dispositivos Windows 10. Para obtener más información acerca de los anillos de implementación, consulta Generar anillos de implementación para las actualizaciones de Windows10.

Consulte la tabla siguiente para obtener ejemplos de anillos de implementación.

ANILLO DE IMPLEMENTACIÓN	TAMAÑO DEL ANILLO	RAMA DE MANTENIMIENTO	APLAZAMIENTO PARA ACTUALIZACIONES DE CARACTERÍSTICAS	APLAZAMIENTO PARA ACTUALIZACIONES DE CALIDAD (REVISIONES DE SEGURIDAD, CONTROLADORES Y OTRAS ACTUALIZACIONES)	PASO DE VALIDACIÓN
Versión preliminar (por ejemplo, dispositivos de prueba o que no sean imprescindibles)	Pequeña	Windows Insider Preview	Ninguno.	Ninguno.	Probar y evaluar la nueva funcionalidad manualmente. Pausar actualizaciones si hay problemas.
Versión publicada (por ejemplo, los dispositivos que usan equipos seleccionados)	Media	Canal semianual	Ninguno.	Ninguno.	Supervisar uso de dispositivos y comentarios de los usuarios. Pausar actualizaciones si hay problemas.
Implementación general (por ejemplo, la mayoría de los dispositivos de la organización)	Grande	Canal semianual	120 días después del lanzamiento.	7-14 días después del lanzamiento.	Supervisar uso de dispositivos y comentarios de los usuarios. Pausar actualizaciones si hay problemas.
Crítica (por ejemplo, los dispositivos en salas de reuniones de ejecutivos)	Pequeña	Canal semianual	180 días después del lanzamiento (aplazamiento máximo para actualizaciones de características).	30 días después del lanzamiento (aplazamiento máximo para actualizaciones de calidad).	Supervisar uso de dispositivos y comentarios de los usuarios.

Configurar cuándo recibe actualizaciones Surface Hub

Cuando hayas determinado los anillos de implementación para los Surface Hubs, configura directivas de aplazamiento de las actualizaciones para cada anillo:

- Para aplazar las actualizaciones de características, establece una directiva Update/DeferFeatureUpdatesPeriodInDays para cada anillo.
- Para aplazar actualizaciones de calidad, establece una directiva Update/DeferQualityUpdatesPeriodInDays para cada anillo.

> **NOTE**
> Si se producen problemas durante el lanzamiento de las actualizaciones, puedes pausarlas mediante Update/PauseFeatureUpdates y Update/PauseQualityUpdates.

Si usas un servidor proxy u otro método para bloquear las direcciones URL

Agregue las siguientes direcciones URL de sitios de confianza de Windows Update a la "lista de permitidos":

- `http(s)://*.update.microsoft.com`
- `http://download.windowsupdate.com`
- `http://windowsupdate.microsoft.com`

Una vez instalada la Actualización de aniversario de Windows 10 Team, puedes quitar estas direcciones para restablecer Surface Hub a su estado anterior.

Ventana de mantenimiento

Para garantizar que el dispositivo está siempre disponible para su uso durante las horas laborables, Surface Hub realiza sus funciones administrativas durante una ventana de mantenimiento especificada. Durante la ventana de mantenimiento, Surface Hub instala automáticamente las actualizaciones a través de Windows Update y reinicia el dispositivo 20 minutos antes del final de la ventana.

Surface Hub sigue estas directrices para aplicar las actualizaciones:

- Instala la actualización durante la siguiente ventana de mantenimiento. Si una reunión está programada para iniciarse durante el mantenimiento o si los sensores de Surface Hub detectan que se está usando el dispositivo, se pospondrá la actualización pendiente hasta la siguiente ventana de mantenimiento.
- Si la siguiente ventana de mantenimiento es después del período de gracia especificado de la actualización, el dispositivo calculará la siguiente ranura disponible durante las horas laborables usando el tiempo estimado de instalación a partir de los metadatos de la actualización. Continuará posponiendo la actualización si se ha programado una reunión o si los sensores de Surface Hub detectan que el dispositivo esté en uso.
- Si la siguiente ventana de mantenimiento **no** supera el período de gracia de la actualización, el Surface Hub seguirá pospuesto la actualización.
- Si se necesita reiniciar, el Surface Hub se reiniciará automáticamente durante la siguiente ventana de mantenimiento.

> **NOTE**
> Reserva tiempo para las actualizaciones cuando configures por primera vez tu Surface Hub. Por ejemplo, un trabajo pendiente de definiciones de virus puede estar disponible y deberá instalarse inmediatamente.

Se establece una ventana de mantenimiento predeterminada para todos los Surface Hubs nuevos:

- **Hora de Inicio:** 2:00 AM
- **Duración:** 2 horas

Para cambiar manualmente la ventana de mantenimiento:

1. Abre **Configuración** en tu Surface Hub.
2. Ve a **Actualización y seguridad** > **Windows Update** > **Opciones avanzadas**.
3. En **Horas de mantenimiento**, selecciona **Cambiar**.

Para cambiar la ventana de mantenimiento con MDM, establezca el nodo **MaintenanceHoursSimple** en el proveedor de servicio de configuración de SurfaceHub. Consulta Administrar la configuración con un proveedor de MDM para obtener más información.

Más información

- Entrada de blog: mantenimiento, vuelo y administración de actualizaciones de Surface Hub (con Intune, por

supuesto)

Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Miracast sobre infraestructura

12/01/2022 • 3 minutes to read

En Windows 10, versión 1703, Microsoft ha ampliado la capacidad de enviar una emisión de Miracast a través de una red local, en lugar de a través de un vínculo directo inalámbrico. Esta funcionalidad se basa en el Protocolo de establecimiento de conexión de Miracast a través de infraestructura (MS-MICE).

Miracast a través de infraestructura ofrece una serie de ventajas:

- Windows detecta automáticamente cuándo se puede enviar la emisión de vídeo a través de esta ruta.
- Windows solo elige esta ruta si la conexión se realiza a través de Ethernet o de una red Wi-Fi segura.
- Los usuarios no tienen que cambiar la forma en que se conectan al receptor de Miracast. Usan la misma experiencia del usuario que en las conexiones de Miracast estándar.
- No es necesario realizar ningún cambio en los controladores inalámbricos existentes ni en el hardware del equipo.
- Funciona bien con el hardware inalámbrico más antiguo que no se haya optimizado para Miracast a través de Wi-Fi Direct.
- Aprovecha la conexión existente, lo que reduce el tiempo de conexión y ofrece una emisión muy estable.

Cómo funciona

Los usuarios intentan conectarse a un receptor Miracast a través de su Wi-Fi como lo hacían anteriormente. Cuando se llena la lista de receptores de Miracast, Windows 10 identificará el receptor que puede admitir una conexión a través de la infraestructura. Cuando el usuario selecciona un receptor de Miracast, Windows 10 intentará resolver el nombre de host del dispositivo a través de DNS estándar y de DNS multidifusión (mDNS). Si el nombre no se puede resolver a través de ninguno de estos métodos DNS, Windows 10 recurrirá a establecer la sesión de Miracast con la conexión de Wi-Fi Direct estándar.

> **NOTE**
> Para obtener más información sobre la secuencia de negociación de conexión, vea Miracast over Infrastructure Connection Establishment Protocol (MS-MICE)

Habilitar Miracast a través de la infraestructura

Si tienes un dispositivo Surface Hub u otro dispositivo con Windows 10 que se ha actualizado a Windows 10, versión 1703, tendrás automáticamente esta nueva característica. Para poder aprovecharla en el entorno, debes asegurarte de que se cumplan las siguientes condiciones en la implementación:

- Surface Hub o el dispositivo (PC o teléfono con Windows) debe ejecutar Windows 10, versión 1703.
- Puerto TCP abierto: **7250**.
- Surface Hub o un PC Windows se puede emplear como *receptor* de Miracast a través de la infraestructura. Un equipo o teléfono con Windows se puede emplear como *origen* de Miracast a través de la infraestructura.
  - Para que funcione como receptor de Miracast, Surface Hub o el dispositivo debe estar conectado a la red de empresa a través de Ethernet o de una conexión Wi-Fi segura (por ejemplo, con seguridad WPA2-PSK o WPA2-Enterprise). Si el Surface Hub o dispositivo está conectado a una conexión Wi-Fi abierta, Miracast sobre infraestructura se deshabilitará a sí mismo.
  - Para servir de origen de Miracast, el equipo o teléfono con Windows debe estar conectado a la misma red de empresa a través de Ethernet o de una conexión Wi-Fi segura.

- El nombre de host DNS (nombre de dispositivo) del Surface Hub o dispositivo debe resolverse a través de los servidores DNS. Puedes lograrlo permitiendo que Surface Hub se registre automáticamente a través de DNS dinámico, o crear manualmente un registro A o AAAA para el nombre de host de Surface Hub.
- Los equipos con Windows 10 deben estar conectados a la misma red de empresa a través de Ethernet o de una conexión Wi-Fi segura.

Es importante tener en cuenta que Miracast a través de la infraestructura no es un sustituto de Miracast estándar. Por el contrario, la funcionalidad es complementaria y ofrece ventajas a los usuarios que forman parte de la red de empresa. Los usuarios invitados en una determinada ubicación que no tengan acceso a la red de empresa seguirán conectándose mediante el método de conexión Wi-Fi Direct.

La opción de configuración **InBoxApps/WirelessProjection/PinRequired** en el proveedor de servicios de configuración (CSP) de SurfaceHub no es necesaria para Miracast a través de la infraestructura. Esto es porque Miracast a través de la infraestructura solo funciona si ambos dispositivos están conectados a la misma red de empresa. De este modo, se elimina de Miracast la restricción de seguridad que faltaba anteriormente. Te recomendamos que sigas usando esta opción de configuración (si la usabas anteriormente), ya que Miracast recurrirá a Miracast normal si la conexión a través de la infraestructura no funciona.

Preguntas más frecuentes

¿Por qué todavía necesito Wi-Fi usar Miracast sobre la infraestructura?
Las solicitudes de detección para identificar Miracast receptores solo se pueden producir a través del Wi-Fi adaptador. Una vez identificados los receptores, Windows 10 puede intentar la conexión a la red.

Guardar la clave de BitLocker (Surface Hub)

12/01/2022 • 2 minutes to read

Cada Microsoft Surface Hub se configura automáticamente con el software de cifrado de unidad de BitLocker. Microsoft recomienda encarecidamente que te asegures de hacer una copia de seguridad de las claves de recuperación de BitLocker.

Hay varias maneras de administrar la clave de BitLocker en Surface Hub.

1. Si uniste Surface Hub a un dominio, el dispositivo realizará una copia de seguridad de la clave del dominio y la almacenará en el objeto del equipo.

   Si no encuentras la clave de BitLocker después de unir el dispositivo a un dominio, es probable que tu esquema de Active Directory no admita la copia de seguridad de la clave de BitLocker. Si no quieres cambiar el esquema, puedes guardar la clave de BitLocker yendo a Configuración y siguiendo el procedimiento para usar una cuenta de administrador local, lo que se detallará más adelante en esta lista.

2. Si has unido Surface Hub a Azure Active Directory (Azure AD), la clave de BitLocker se almacenará en la cuenta usada para unir el dispositivo.

3. Si está usando una cuenta de administrador local para administrar el dispositivo, puede guardarla en la aplicación **configuración** y navegar para **Actualizar &** la > **recuperación**de seguridad. Inserta una unidad USB y selecciona la opción para guardar la clave de BitLocker. La clave se guardará en un archivo de texto en la unidad USB.

Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Actualizar el firmware del lápiz en Surface Hub 2S

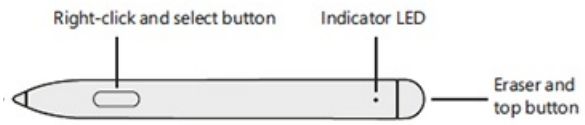
12/01/2022 • 3 minutes to read

Puede actualizar el firmware en Surface Hub 2 pen desde Windows Update for Business o descargando la actualización de firmware en un equipo independiente. El firmware actualizado está disponible desde Windows actualización a partir del 26 de febrero de 2020.

Actualizar el firmware del lápiz con Windows update para empresas

En esta sección se describe cómo actualizar el firmware del lápiz a través de los ciclos de mantenimiento automatizados de Windows Update, configurados de forma predeterminada para que se produzcan cada noche a las 3 a. m. Deberá planear dos ciclos de mantenimiento para completar antes de aplicar la actualización al Surface Hub 2 plumas. Como alternativa, como cualquier otra actualización, puede usar Windows Update for Business (WUfB) para aplicar el firmware del lápiz. Para obtener más información, vea Managing Windows updates on Surface Hub.

1. Asegúrese de Surface Hub 2 plumas esté emparejada a Surface Hub 2S: mantenga presionado el botón superior hasta que la luz LED indicadora blanca comience a parpadear. ****

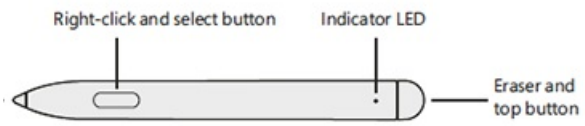


2. On Surface Hub, login as an Admin, open **Configuración**, and then scan for new Bluetooth devices.
3. Seleccione el lápiz para completar el proceso de emparejamiento.
4. Presione el **botón** superior del lápiz para aplicar la actualización. Puede tardar hasta dos horas en completarse.

Actualizar el firmware del lápiz descargando en un equipo independiente

Puede actualizar el firmware en un Surface Hub 2 pen desde un equipo independiente que ejecute Windows 10. Este método también permite comprobar que el firmware del lápiz se actualizó correctamente a la versión más reciente.

1. Empareja el Surface Hub 2 plumas al equipo compatible con Bluetooth: **** mantén presionado el botón superior hasta que la luz LED indicadora blanca comience a parpadear.



2. En el equipo, busca nuevos Bluetooth dispositivos.
3. Seleccione el lápiz para completar el proceso de emparejamiento.
4. Desconecte el resto Surface Hub 2 lápices antes de iniciar una nueva actualización.
5. Descargue la herramienta Surface Hub actualización de firmware de 2 plumas en el equipo.

6. Ejecute **PenCfu.exe.** El progreso de instalación se muestra en la herramienta. Puede tardar varios minutos en finalizar la actualización.

Comprobar la versión de firmware de Surface Hub 2 plumas

1. Ejecute **get_version.bat** y presione el **botón superior** del lápiz.
2. La herramienta mostrará la versión de firmware del lápiz.

   Por ejemplo:

   - El firmware antiguo es 468.2727.368
   - El nuevo firmware es 468.3347.368

Opciones de línea de comandos

Puede ejecutar Surface Hub 2 Pen Firmware Update Tool (PenCfu.exe) desde la línea de comandos.

1. Empareja el lápiz con el equipo y haz clic en **el botón superior** del lápiz.
2. Haga doble ** clicPenCfu.exe** para iniciar la actualización de firmware. Tenga en cuenta que el archivo de configuración y los archivos de imagen de firmware deben almacenarse en la misma carpeta que la herramienta.
3. Para obtener opciones adicionales, ** ejecutePenCfu.exe -h para** mostrar los parámetros disponibles, como se muestra en la tabla siguiente.

   Por ejemplo: `PenCfu.exe -h`
4. Escriba **Ctrl+C para** apagar la herramienta de forma segura.

COMANDO	DESCRIPCIÓN
Ayuda de -h	Mostrar ayuda y salida de la interfaz de línea de comandos de la herramienta.
-v version	Mostrar versión y salida de la herramienta.
-l log-filter	Establecer un nivel de filtro para el archivo de registro. Los mensajes de registro tienen 4 niveles posibles: DEBUG (más bajo), INFO, WARNING y ERROR (más alto). Al establecer un nivel de filtro de registro, los mensajes de registro solo se filtran en mensajes con el mismo nivel o superior. Por ejemplo, si el nivel de filtro está establecido en WARNING, solo se registrarán los mensajes WARNING y ERROR. De forma predeterminada, esta opción se establece en OFF, que deshabilita el registro.
-g get-version	Si se especifica, la herramienta solo recibirá la versión FW del lápiz conectado que coincida con el archivo de configuración almacenado en la misma carpeta que la herramienta.

Accesibilidad (Surface Hub)

12/01/2022 • 2 minutes to read

Microsoft Surface Hub tiene las mismas opciones de accesibilidad que Windows10.

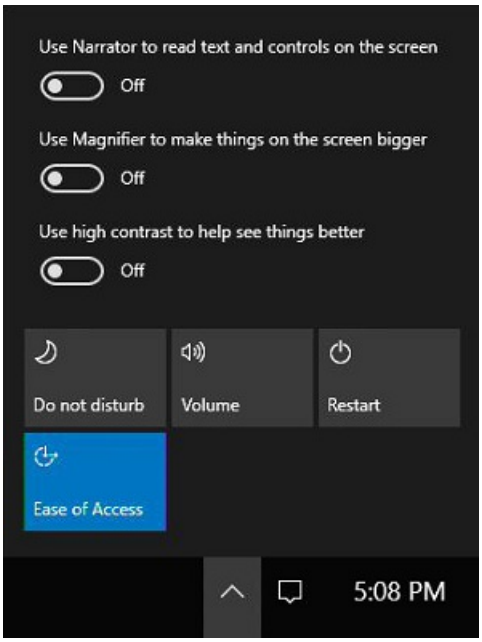
Configuración de accesibilidad predeterminada

La lista completa de la configuración de accesibilidad está disponible para los administradores de TI en la aplicación **Configuración**. La configuración de accesibilidad predeterminada de Surface Hub incluye:

CARACTERÍSTICA DE ACCESIBILIDAD	CONFIGURACIÓN PREDETERMINADA
Lupa	Desactivado
Contraste alto	Ningún tema seleccionado
Subtítulos	Valores predeterminados seleccionados para Fuente y Fondo y ventana
Teclado	El **teclado en pantalla**, las **teclas especiales**, las **teclas de alternancia**y las **teclas filtro** están desactivados.
Mouse	Valores predeterminados seleccionados para el **tamaño del puntero**, el **color del puntero** y las **teclas de mouse**.
Otras opciones	Valores predeterminados seleccionados para **Opciones visuales** e **Comentarios táctiles**.

La característica de accesibilidad Narrador no está disponible en la aplicación **Configuración**. De manera predeterminada, el Narrador está desactivado. Para cambiar la configuración predeterminada del Narrador, lleva a cabo los pasos con un teclado y mouse.

1. Descarta la pantalla de inicio de sesión.
2. Abre **Acciones rápidas** > **Accesibilidad** de la barra de estado.



3. Activa el Narrador.
4. Haz clic en **Conmutador de tareas**.
5. Selecciona **Configuración del Narrador** en Conmutador de tareas. Ahora puedes editar la configuración predeterminada de Narrador.

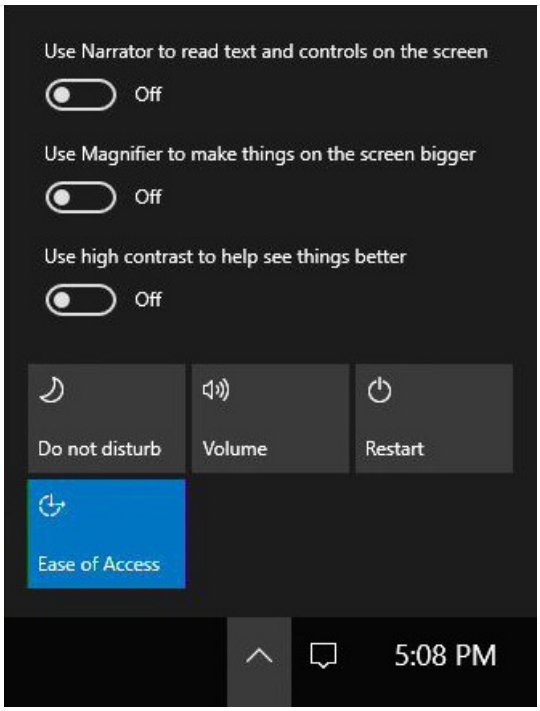
Además, estas aplicaciones y características de accesibilidad vuelven a la configuración predeterminada cuando los usuarios presionan Finalizar sesión:

- Narrador
- Lupa
- Contraste alto
- Teclas de filtro
- Teclas especiales
- Teclas de alternancia
- Teclas del mouse

Cambiar la configuración de accesibilidad durante una reunión

Durante una reunión, los usuarios pueden alternar las aplicaciones y las características de accesibilidad de un par de formas:

- Métodos abreviados de teclado
- **Acciones rápidas** > **Accesibilidad** de la barra de estado



Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Introducción a la seguridad de Surface Hub

12/01/2022 • 11 minutes to read

Surface Hub ofrece una experiencia similar a la de un dispositivo bloqueado con un firmware de plataforma personalizado que ejecuta el sistema operativo Windows 10 Team. El dispositivo resultante adopta la filosofía tradicional de quiosco seguro de "uso único" en el que "solo ejecuta lo que necesita" y ofrece un enfoque moderno al respecto. Diseñado para dar soporte a una experiencia de usuario colaborativa rica, Surface Hub se protege frente a las amenazas de seguridad en constante evolución.

Creado a partir de Windows 10, Surface Hub ofrece seguridad moderna a nivel empresarial, lo que permite a los administradores de TI aplicar la protección de datos con BitLocker, el Módulo de plataforma segura 2.0 (TPM), además de seguridad con tecnología de la nube con Windows Defender (también conocido como Microsoft Defender).

Seguridad de Defensa en profundidad

Los protocolos de seguridad se ponen en marcha en cuanto se enciende Surface Hub. Empezando por el nivel de firmware, Surface Hub solo cargará el sistema operativo y sus componentes en respuesta a las múltiples comprobaciones de seguridad. Surface Hub emplea una estrategia denominada Defensa en profundidad que involucra organizar en capas subcomponentes de defensa independientes para proteger todo el sistema en caso de fallo parcial. Esta práctica del sector ha demostrado ser muy eficaz en la mitigación de posibles ataques unilaterales y de puntos débiles en los subcomponentes.

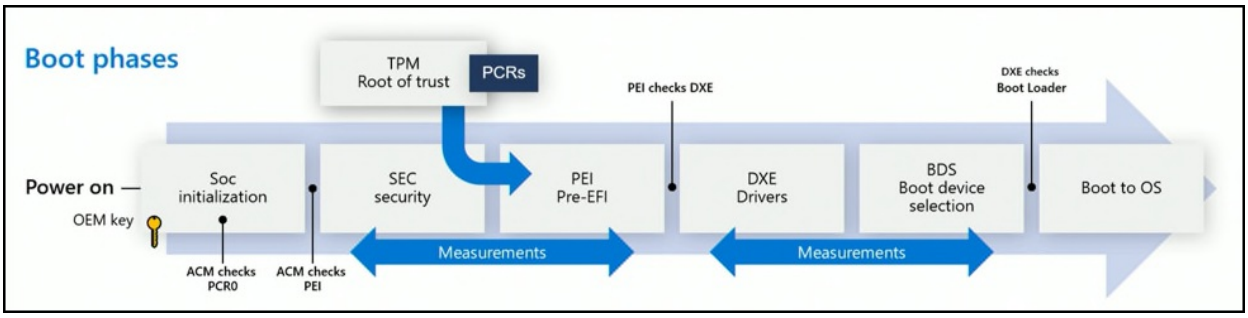
Microsoft ha configurado la Unified Extensible Firmware Interface (UEFI) de forma estática y segura para arrancar únicamente un sistema operativo Windows 10 Team autenticado desde un almacenamiento interno. La firma de todas las líneas de código que se ejecuten en Surface Hub se comprueba antes de su ejecución. Solo las aplicaciones firmadas por Microsoft, ya sea como parte del sistema operativo o instaladas desde la Microsoft Store, pueden ejecutarse en Surface Hub. El código o las aplicaciones que no cumplan estos requisitos se bloquearán.

Los sistemas de seguridad de Surface Hub incluyen lo siguiente:

- **Defensas durante el arranque.** Solo se cargan los componentes del sistema operativo de confianza de Surface Hub.
- **Defensas de sistema operativo.** Se protege contra la ejecución de código o software no intencionado o malintencionado.
- **Defensas de la interfaz de usuario.** Se ofrece una interfaz de usuario segura para los usuarios finales, lo que les impide el acceso a actividades potencialmente peligrosas como iniciar archivos ejecutables desde la línea de comandos.

Defensas durante el arranque

El SoC tiene un procesador de seguridad independiente de cualquier otro núcleo. La primera vez que inicie Surface Hub, solo se iniciará el procesador de seguridad antes de que se pueda cargar cualquier otro elemento.



Arranque seguro

El Arranque seguro se usa para comprobar que los componentes del proceso de inicio, incluidos los controladores y el sistema operativo, se validan con una base de datos de firmas válidas y conocidas. En Surface Hub, debe validarse primero una firma específica de la plataforma antes de que se pueda cargar el sistema operativo de Windows Team autorizado. Esto ayuda a evitar que se produzcan ataques de un sistema clonado o modificado en el que se ejecuta código malintencionado oculto en lo que parece ser una experiencia de usuario normal. Para obtener más información, consulte Información sobre el arranque seguro.

Defensas de sistema operativo

Una vez que se comprueba el sistema operativo como originario de Microsoft y Surface Hub completa satisfactoriamente el proceso de inicio, el dispositivo inspecciona el código ejecutable. Nuestro método para proteger el sistema operativo consiste en identificar la firma de código de todos los archivos ejecutables, de modo que solo los que superen las restricciones se carguen en tiempo de ejecución. Este método de firma de código permite al sistema operativo comprobar el autor y confirmar que el código no se ha modificado antes de ejecutarse en el dispositivo.

Surface Hub usa una característica de firma de código conocida como Integridad de código del modo usuario (UMCI) en el Control de aplicaciones de Windows (anteriormente conocido como Device Guard). Se configuran las opciones de la directiva de tal modo que solo admita aplicaciones que cumplan uno de estos requisitos:

- Aplicaciones de Plataforma universal de Windows (Microsoft Store) que están certificadas oficialmente.
- Las aplicaciones firmadas con la exclusiva entidad de certificación (CA) raíz de producción de Microsoft, que solo pueden firmar los empleados de Microsoft con el acceso autorizado a estos certificados.
- Aplicaciones firmadas con la exclusiva Raíz C de producción de Surface Hub.

El archivo de configuración se firma con la entidad de certificación de raíz de producción de Microsoft diseñada para evitar que un tercero pueda quitar o modificar las restricciones. En este momento dado, los demás archivos ejecutables simplemente se bloquean en el nivel de tiempo de ejecución del sistema operativo y se evita que utilicen recursos de procesamiento. Esta reducción de la superficie de ataque ofrece las siguientes protecciones:

- Ningún modo de documento heredado
- Ningún motor de scripts heredado
- Ningún lenguaje de marcado de vectores
- Ningún objeto auxiliar de explorador
- Ningún control de ActiveX

Además de bloquear el código sin firma o firmado de forma incorrecta mediante UMCI, Surface Hub usa el Control de aplicaciones de Windows para bloquear componentes de Windows como el Símbolo del sistema, PowerShell y el Administrador de tareas. Este sistema de seguridad refleja una característica de diseño clave de Surface Hub como dispositivo de computación seguro. Para obtener más información, consulte:

- Introducción al control de aplicaciones
- Control de aplicaciones de Windows Defender y protección basada en la virtualización de la integridad del código

Defensas de la interfaz de usuario

Aunque las defensas en tiempo de arranque y las protecciones de bloqueo del sistema operativo proporcionan seguridad fundamental, la interfaz de usuario ofrece un nivel adicional que se ha diseñado para reducir los riesgos. Para impedir que algún código malintencionado llegue al dispositivo a través de los controladores, Surface Hub no descarga controladores avanzados para dispositivos Plug and Play (PnP). Los dispositivos que aprovechan los controladores básicos, como las unidades flash USB o los periféricos de Surface Hub certificados (altavoces, micrófonos y cámaras) funcionan como se espera, pero los sistemas avanzados, como las impresoras, no lo harán.

Las defensas de la interfaz de usuario también simplifican la interfaz de usuario y evitan la ejecución de código o software malintencionado. Los siguientes elementos de la interfaz de usuario de Surface Hub separan por capas la seguridad principal proporcionada por la firma de código:

- **Explorador de archivos.** Surface Hub tiene un Explorador de archivos personalizado que permite acceder rápidamente a las carpetas Música, Vídeos, Documentos, Imágenes y Descargas, sin tener que revelar a los usuarios los archivos de programa o del sistema. No se puede acceder a otras ubicaciones de la unidad de disco duro local a través del Explorador de archivos. Además, muchos tipos de archivos ejecutables, como. exe y. msi, no se pueden ejecutar, lo que proporciona otro nivel de seguridad frente a ejecutables potencialmente maliciosos.
- **Inicio y Todas las aplicaciones.** Los componentes Inicio y Todas las aplicaciones de Surface Hub no exponen el acceso al Símbolo del sistema, PowerShell u otros componentes de Windows bloqueados mediante el Control de aplicaciones. Además, la funcionalidad de ejecución de Windows, a la que generalmente se accede en equipos PC desde el cuadro de búsqueda, está desactivada para Surface Hub.

Mejoras en la seguridad de Surface Hub 2S

Aunque Surface Hub y Surface Hub 2S ejecutan el mismo sistema operativo, algunas características exclusivas de Surface Hub 2S proporcionan capacidades de administración y seguridad adicionales que permiten a los administradores de TI realizar las siguientes tareas:

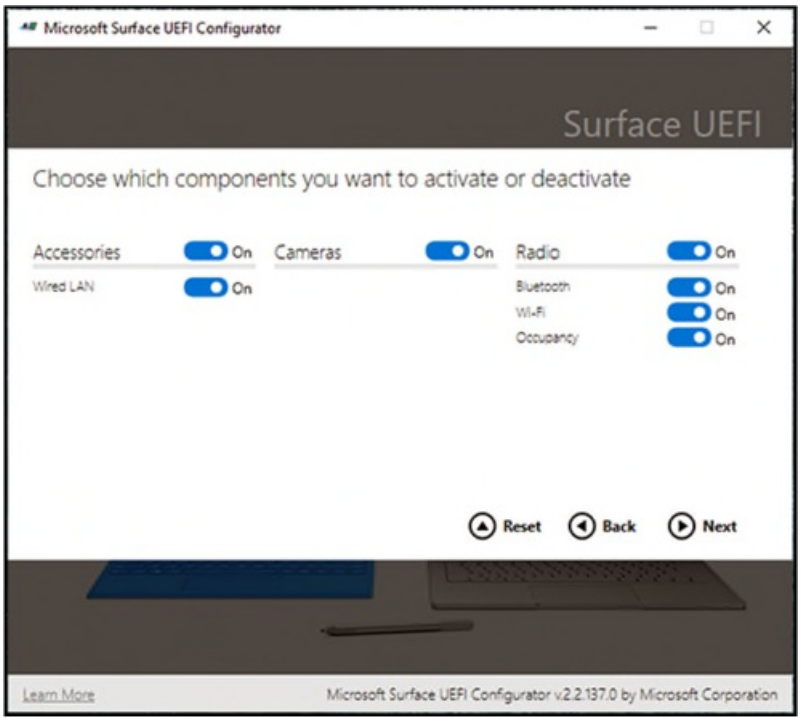
- Administrar la configuración de UEFI con SEMM
- Recuperar Hub con un USB de arranque
- Reforzar la cuenta del dispositivo mediante la rotación de contraseñas

Administrar la configuración de UEFI con SEMM

UEFI es una interfaz situada entre las partes de la plataforma de hardware subyacente y el sistema operativo. En Surface Hub, una implementación personalizada de UEFI permite tener control específico sobre esta configuración y evita que cualquier entidad que no sea de Microsoft cambie la configuración de UEFI del dispositivo, o el arranque desde una unidad extraíble para modificar o cambiar el sistema operativo.

En un nivel superior, durante el proceso de aprovisionamiento de fábrica, la UEFI de Surface Hub se configura previamente para que permita el arranque seguro y se establece que arranque únicamente desde una unidad interna de estado sólido (SSD), con el acceso a los menús de UEFI bloqueado y los accesos directos eliminados. Esto sella el acceso a la UEFI y garantiza que el dispositivo solo pueda arrancar en el sistema operativo Windows Team instalado en Surface Hub.

Cuando se administra a través del Surface Enterprise Management Mode (SEMM) de Microsoft, los administradores de TI pueden implementar la configuración de UEFI en los dispositivos Hub de toda una organización. Esto incluye la posibilidad de habilitar o deshabilitar los componentes de hardware integrados, evitar que los usuarios no autorizados cambien la configuración de UEFI y ajustar la configuración de arranque.



Los administradores pueden implementar SEMM y los dispositivos inscritos en Surface Hub 2S con el Configurador de UEFI de Surface de Microsoft descargable. Para obtener más información, consulte Proteger y administrar Surface Hub 2S con SEMM y UEFI. SEMM, que está protegido por un certificado para salvaguardar la configuración frente a la alteración o eliminación no autorizadas, permite la administración de los siguientes componentes:

- LAN de cable
- Cámara
- Bluetooth
- Wi-Fi
- Sensor de ocupación
- IPv6 para el arranque PXE
- Arranque alternativo
- Bloqueo de orden de arranque
- Arranque desde USB
- Interfaz de página de información de UEFI
  - Dispositivos
  - Arranque
  - Fecha y hora

Recuperar Hub con un USB de arranque

Surface Hub 2S permite a los administradores devolver el dispositivo a la configuración de fábrica con una imagen de recuperación en tan solo 20 minutos. Normalmente, solo sería necesario llevar a cabo esta acción si Surface Hub deja de funcionar. La recuperación también es útil si ha perdido la clave de BitLocker o ya no tiene credenciales de administrador para la aplicación Configuración.

Reforzar la cuenta del dispositivo mediante la rotación de contraseñas

Surface Hub usa una cuenta de dispositivo, también denominada "cuenta de sala", para autenticar con Exchange, Microsoft Teams y otros servicios. Cuando se habilita la rotación de contraseñas, Hub 2S genera automáticamente una nueva contraseña cada 7 días, que se compone de entre 15 y 32 caracteres con una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Como nadie conoce la contraseña, la rotación de contraseñas de la cuenta del dispositivo mitiga eficazmente el riesgo asociado a errores humanos y posibles ataques de seguridad mediante ingeniería social.

Seguridad empresarial de Windows 10

Además de las configuraciones y características específicas de Surface Hub que se tratan en este documento, Surface Hub también usa las características de seguridad estándares de Windows 10. Entre ellos se incluyen los siguientes:

- **BitLocker**. El SSD de Surface Hub está equipado con BitLocker para proteger los datos en el dispositivo. Su configuración sigue los estándares del sector. Para obtener más información, consulte Introducción a BitLocker.
- **Windows Defender.** El motor antimalware de Windows Defender se ejecuta de forma continua en Surface Hub y corrige automáticamente las amenazas que se encuentren en Surface Hub. El motor de Windows Defender recibe actualizaciones automáticamente y se administra mediante herramientas de administración remota para administradores de TI. El motor de Windows Defender es un ejemplo perfecto de nuestro enfoque de Defensa en profundidad: si el malware puede encontrar una manera de evitar nuestra solución básica de seguridad basada en código firmado, se detectará aquí. Para obtener más información, consulte Control de aplicaciones de Windows Defender y protección basada en la virtualización de la integridad del código.
- **Controladores Plug and Play.** Para impedir que un código malintencionado llegue al dispositivo a través de los controladores, Surface Hub no descarga controladores avanzados para dispositivos PnP. Esto permite que los dispositivos que usan controladores básicos, como las unidades flash USB, funcionen como se espera, a la vez que se bloquean sistemas más avanzados como impresoras.
- **Módulo de plataforma segura 2.0** Surface Hub tiene un módulo de plataforma segura diferenciado (dTPM) estándar del sector para generar y almacenar claves criptográficas y hashes. El dTPM protege las claves que se usan para la comprobación de las fases de arranque, la clave maestra de BitLocker, la clave de inicio de sesión sin contraseña y mucho más. El dTPM cumple la certificación FIPS 140-2 de nivel 2, el estándar de seguridad de equipos de la administración de Estados Unidos, y cumple con la certificación de criterios comunes usada en todo el mundo.

Seguridad inalámbrica para Surface Hub

Surface Hub usa la tecnología Wi-Fi Direct o Miracast y los estándares 802.11, Acceso protegido Wi-Fi (WPA2) y Wireless Protected Setup (WPS) asociados. Dado que el dispositivo solo admite WPS (en lugar de clave precompartida de WPA2 (PSK) o WPA2 Enterprise), los problemas que se asociaban tradicionalmente con el cifrado 802.11 se simplificaron por diseño.

Miracast pertenece al estándar de Wi-Fi Display, que también es compatible con el protocolo de Wi-Fi Direct. Estos estándares son compatibles con dispositivos móviles modernos para colaboración y uso compartido de pantalla.

Wi-Fi Direct o Wi-Fi "Punto a punto" (P2P) es un estándar publicado por Wi-Fi Alliance para las redes "ad hoc". Esto permite que los dispositivos compatibles se puedan comunicar directamente y creen grupos de redes sin necesidad de un punto de acceso Wi-Fi tradicional o una conexión a Internet.

La seguridad de Wi-Fi Direct la proporciona WPA2 con el estándar WPS. Los dispositivos pueden autenticarse con un PIN numérico, un botón de comando físico o virtual, o un mensaje fuera de banda mediante transmisión de datos en proximidad. Surface Hub es compatible de forma predeterminada con el botón de comando y con métodos PIN. Para obtener más información, consulte Cómo gestiona Surface Hub los problemas de seguridad de Wi-Fi Direct.

Obtén más información

- Introducción al arranque seguro
- Introducción a BitLocker

- Introducción al control de aplicaciones
- Proteger y administrar Surface Hub 2S con SEMM y UEFI
- Cómo gestiona Surface Hub los problemas de seguridad de Wi-Fi Direct
- Control de aplicaciones de Windows Defender y protección basada en la virtualización de la integridad del código
- Herramientas de Surface para TI
- FIPS 140-2 nivel 2
- Certificación de criterios comunes

Proteger y administrar Surface Hub 2S con SEMM y UEFI

12/01/2022 • 2 minutes to read

Como novedad Surface Hub 2S, puedes usar SEMM para administrar la configuración UEFI del dispositivo. Usa el Configurador UEFI de Microsoft Surface para controlar los siguientes componentes:

- LAN de cable
- Cámaras
- Bluetooth
- Wi-Fi
- Sensor de ocupación

Usa el Configurador UEFI de Microsoft Surface para activar o desactivar la siguiente configuración de UEFI:

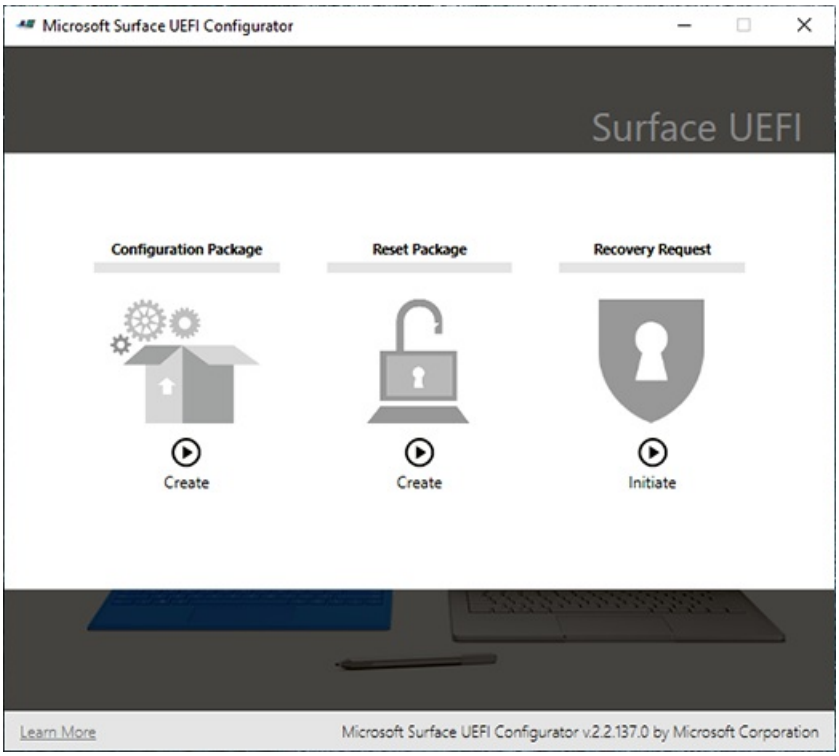
- Arranque
  - IPv6 para el arranque PXE
  - Arranque alternativo
  - Bloqueo de orden de arranque
  - Arranque desde USB
- Página principal uefi
  - Dispositivos
  - Arranque
  - Fecha y hora

Crear imagen de configuración de UEFI

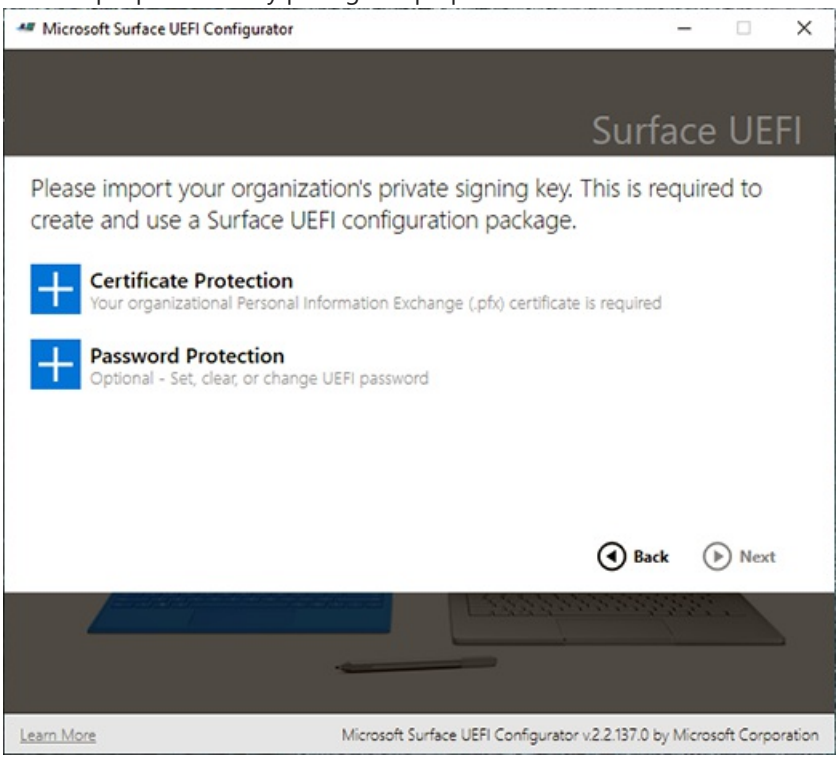
A diferencia de otros dispositivos Surface, no puedes usar un archivo MSI o una imagen win PE para aplicar esta configuración en Surface Hub 2S. En su lugar, debes crear una imagen USB para cargarla en el dispositivo. Para crear una Surface Hub de configuración de UEFI de 2S, descarga e instala la versión más reciente del Configurador UEFI de Microsoft Surface desde la página Herramientas de Surface para TI en el Centro de descarga de Microsoft. Para obtener más información acerca del uso de UEFI y SEMM, consulta Microsoft Surface Enterprise Management Mode.

Para configurar UEFI en Surface Hub 2S

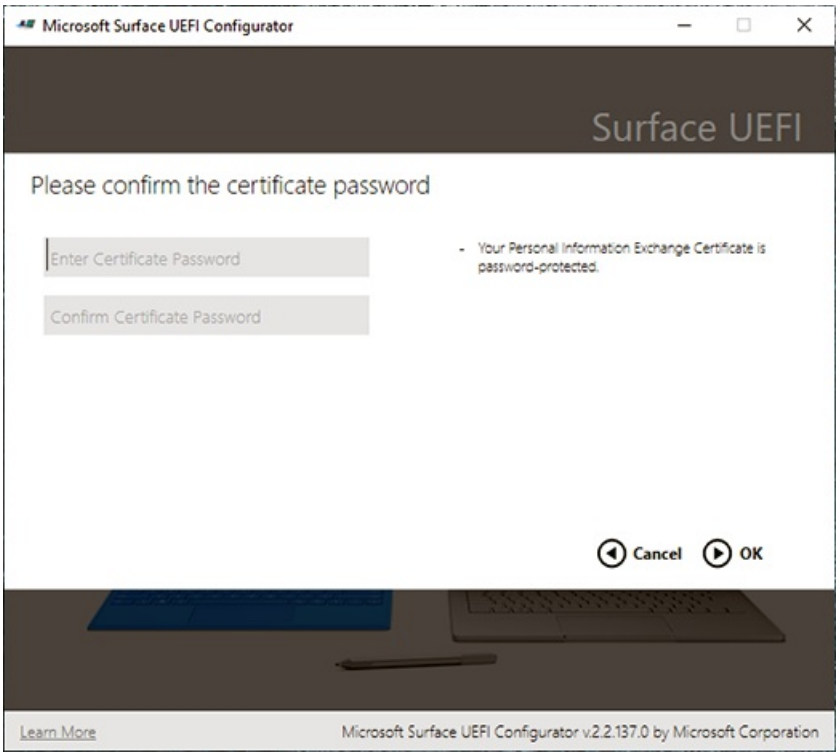
1. Inicie el configurador UEFI y, en la primera pantalla, elija **Paquete de configuración**.



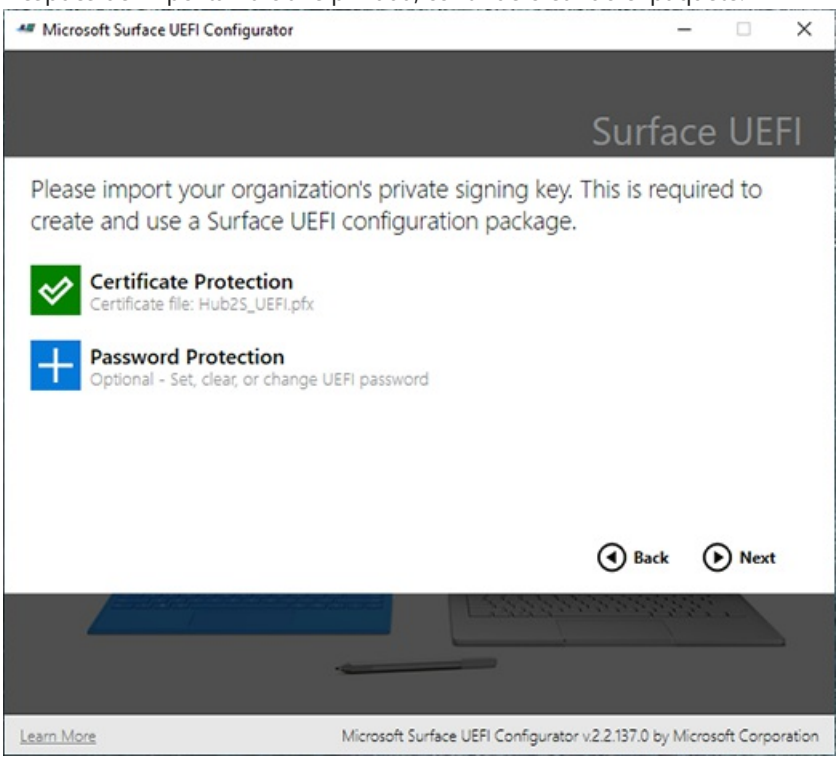
2. Para agregar el certificado al paquete, debe tener un certificado válido con la clave privada en un formato de archivo .pfx para firmar y proteger el paquete. Seleccione **+ Protección de certificados.**



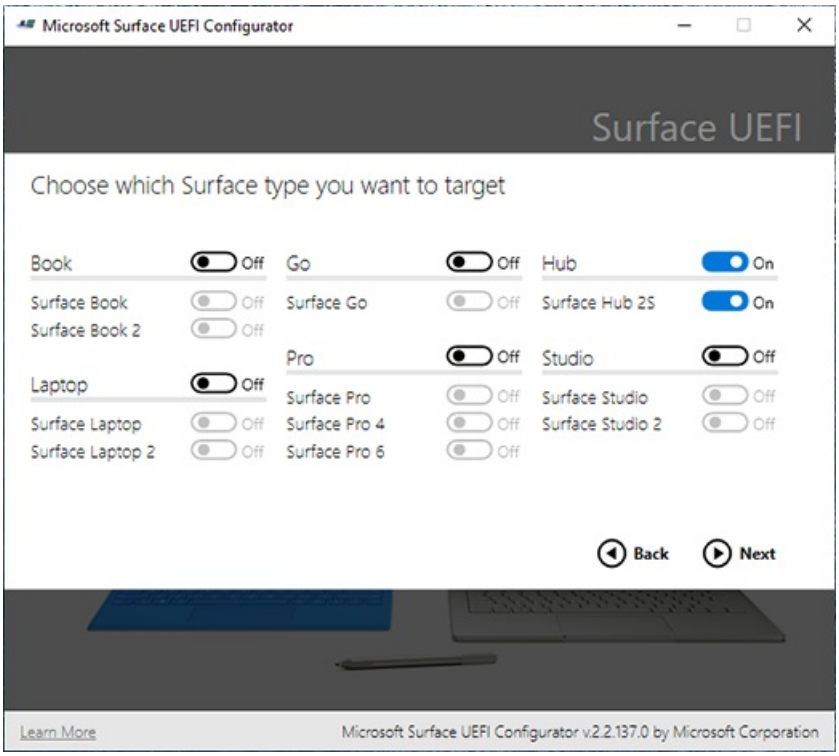
3. Escriba la contraseña de la clave privada del certificado.



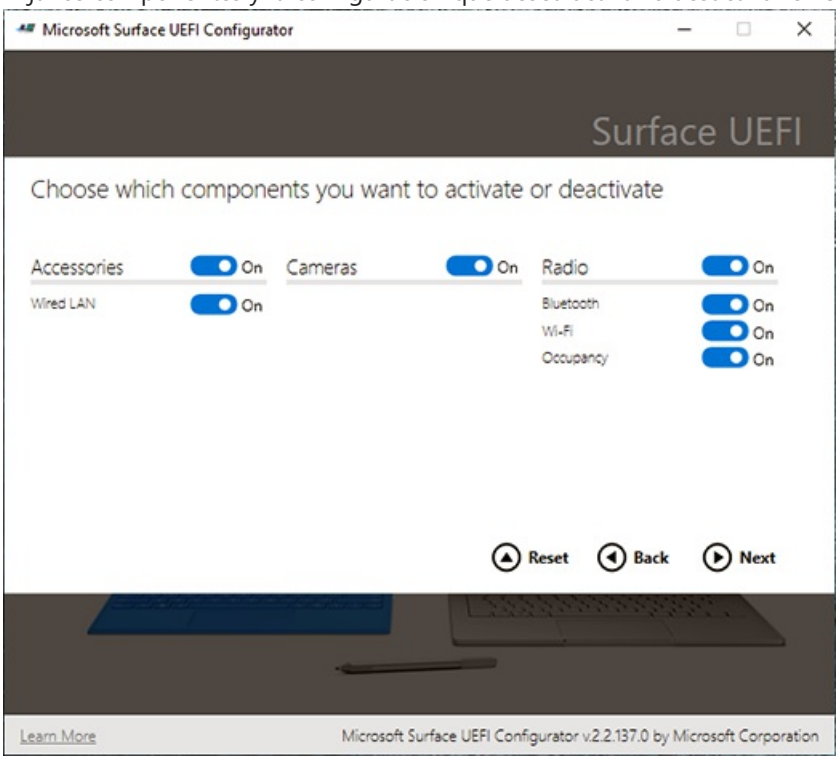
4. Después de importar la clave privada, continúe creando el paquete.



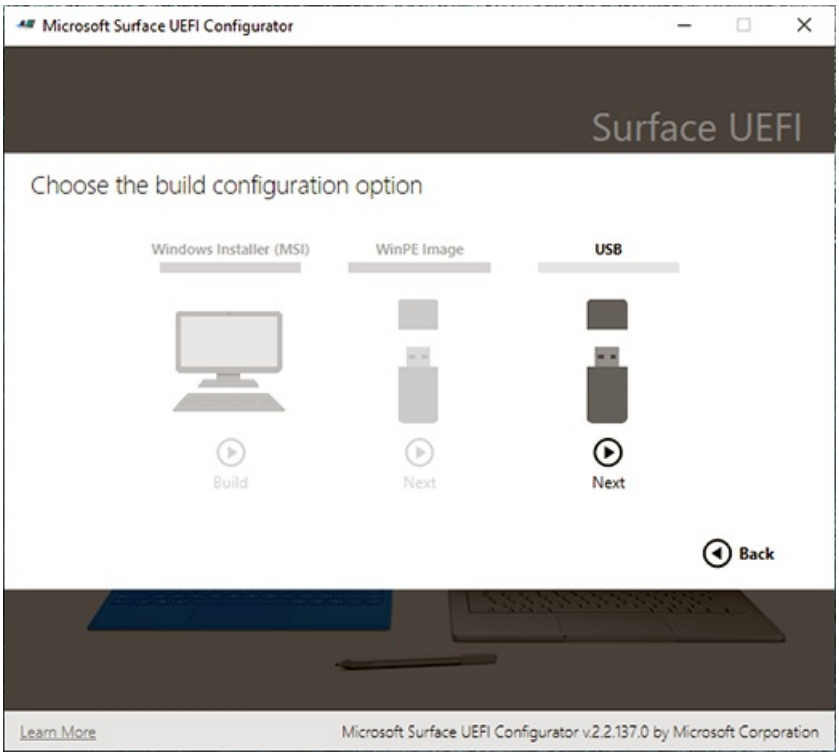
5. Elija **Concentrador** y **Surface Hub 2S** como destino para el paquete de configuración de UEFI.



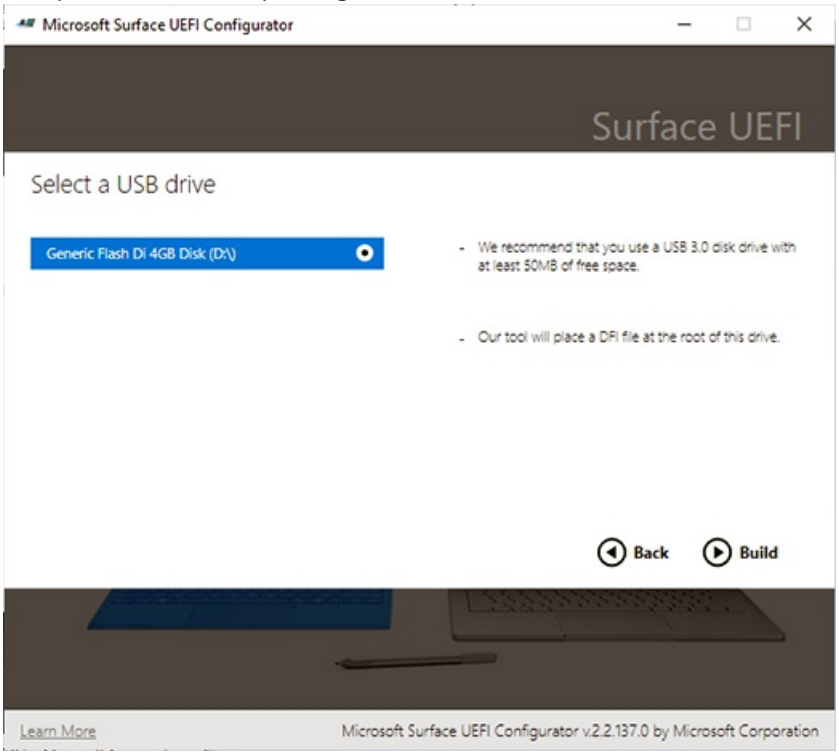
6. Elija los componentes y la configuración que desea activar o desactivar en Surface Hub 2S.



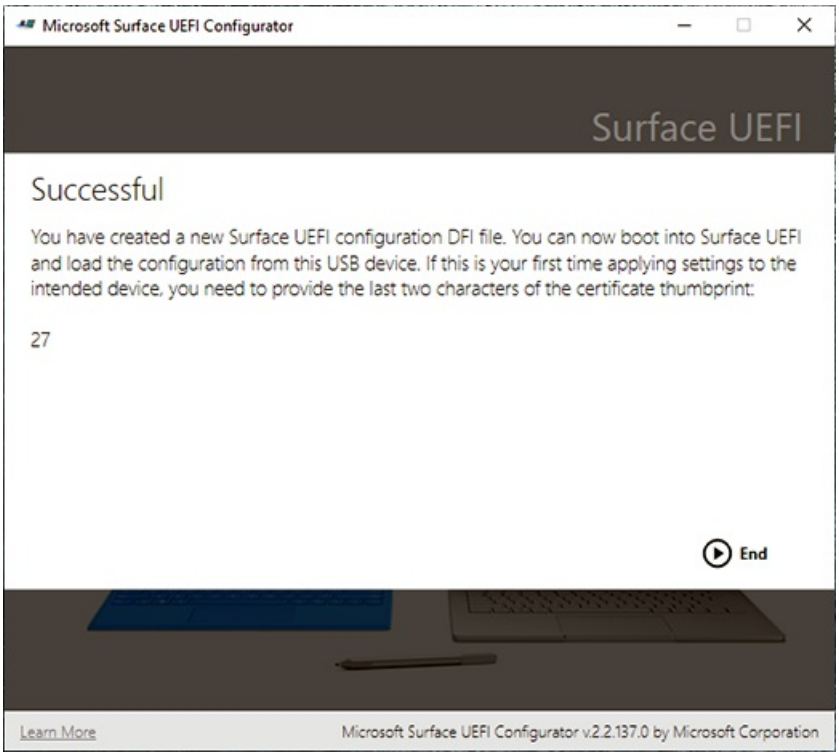
7. Usa la opción USB para exportar el archivo.



8. Inserte y elija la unidad USB que desea usar para este paquete. La unidad USB tendrá formato y perderás cualquier información que tenga en ella.



9. Una vez creado correctamente el paquete, el Configurador mostrará los dos últimos caracteres de la huella digital del certificado. Necesita estos caracteres al importar a la configuración a Surface Hub 2S.



Para arrancar en UEFI

Desactivar Surface Hub 2S. Mantenga presionado el botón **Subir** volumen y presione el **botón de** encendido. Mantenga presionado el botón Subir volumen hasta que aparezca el menú UEFI.

Autenticación moderna en Surface Hub

12/01/2022 • 2 minutes to read

La actualización de Windows 10 Team 2020 agrega compatibilidad con la autenticación moderna de la cuenta del dispositivo Hub en algunos escenarios. Una vez instalada la actualización de 2020, puede migrar desde la autenticación básica heredada para usar las mejoras de seguridad más recientes si la cuenta del dispositivo se autentica a través de Azure Active Directory y el buzón de la cuenta está hospedado en Exchange Online. Con la actualización de 2020, Surface Hub admite protocolos de Exchange Web Services (EWS) y autenticación basada en la Biblioteca de autenticación de Active Directory (ADAL) al sincronizar la cuenta del dispositivo con Exchange Online.

Para las nuevas cuentas basadas en la nube, Surface Hub usa automáticamente la autenticación moderna para conectarse a Exchange Online sin necesidad de configuración adicional más allá de simplemente agregar la cuenta de dispositivo a Surface Hub con el formato alias@contoso.com. No use el formato heredado: Contoso\alias, que no es compatible con la autenticación moderna. Para obtener más información, consulta crear y probar una cuenta de dispositivo.

> **NOTE**
> La autenticación moderna no es compatible con las cuentas locales de Surface Hub. Las cuentas solo deben usar Azure AD para la autenticación.

Configurar el inicio de sesión sin contraseña en Surface Hub

12/01/2022 • 3 minutes to read

El inicio de sesión sin contraseña simplifica el acceso a sus aplicaciones, reuniones y archivos. Surface Hub permite iniciar sesión con la aplicación Microsoft Authenticator y las claves de seguridad fido2 proporcionadas por la organización.

Importante: Este contenido está destinado a los usuarios. Para usar el inicio de sesión sin contraseña, el administrador de TI debe habilitar la autenticación sin contraseña para su organización. Para más información, consulta lo siguiente:

- Habilitar el inicio de sesión de teléfono sin contraseña
- Habilitar el inicio de sesión con clave de seguridad sin contraseña

Configurar el inicio de sesión con Microsoft Authenticator aplicación

Nota: A partir de Windows 10 Team actualización de 2020, los usuarios pueden usar sus alias de correo electrónico preferidos en Azure AD, así como su nombre principal de usuario (UPN), para iniciar sesión con Microsoft Authenticator. Por ejemplo, un usuario puede usar su alias preferido (John.Doe@contoso.com) o su UPN (jdoe@contoso.com) para iniciar sesión.

La Microsoft Authenticator te ayuda a iniciar sesión en Surface Hub usar el dispositivo móvil. Para configurar el inicio de sesión con Microsoft Authenticator:

1. En el dispositivo móvil, descarga la Microsoft Authenticator aplicación.
   - Google Android: en tu dispositivo Android, ve a Google Play para descargar e instalar la Microsoft Authenticator aplicación.
   - Apple iOS: en tu dispositivo Apple iOS, ve a la App Store para descargar e instalar la Microsoft Authenticator aplicación.
2. En el equipo, configura la aplicación Microsoft Authenticator desde la página Información de seguridad de tu cuenta laboral o educativa.
3. Desde la Microsoft Authenticator en tu dispositivo móvil, activa y usa el inicio de sesión del teléfono para tu cuenta laboral o educativa.

Configurar el inicio de sesión con claves de seguridad FIDO2

> **NOTE**
> El inicio de sesión sin contraseña Surface Hub con claves de seguridad FIDO2 requiere la actualización Windows 10 Team 2020.

> **IMPORTANT**
> Surface Hub solo admite claves de seguridad USB.

También puede iniciar sesión en Surface Hub con una clave de seguridad FIDO2 proporcionada por su organización.

Para configurar el inicio de sesión con una clave de seguridad:

1. En el equipo, vaya a la página e inicie sesión en su cuenta laboral https://myprofile.microsoft.com/ o educativa.
2. Selecciona **Información de seguridad** en el panel **** de navegación izquierdo o en el vínculo del bloque Información de seguridad y, a continuación, selecciona **Agregar** método en la página **Información de** seguridad.
3. En la **página Agregar un método,** seleccione Clave **de seguridad** de la lista desplegable y, a continuación, **seleccione Agregar**.
4. En la **página Clave de** seguridad, elija Dispositivo **USB**.
5. Tenga la clave de seguridad lista y seleccione **Siguiente**.
6. En el cuadro de diálogo que aparece, siga las instrucciones para insertar la clave de seguridad, crear o escribir un PIN y realizar el gesto necesario (ya sea biométrico o táctil).
7. En la **página Clave de** seguridad, asigne un nombre a la clave de seguridad y, a continuación, seleccione **Siguiente**.
8. Seleccione **Listo** para completar el proceso.

Inicie sesión en Surface Hub

Una vez que hayas configurado el inicio de sesión sin contraseña, puedes usarlo para facilitar el acceso a tus aplicaciones, reuniones y archivos en el Surface Hub:

- Únase rápidamente a sus reuniones y abra archivos Microsoft 365 recientes. Para obtener más información, vea **Iniciar sesión para ver sus reuniones y archivos.**
- Inicie sesión rápidamente en aplicaciones de Microsoft como Whiteboard, PowerPoint, Word, Excel, OneDrive y Power BI.
- Inicie sesión rápidamente en el nuevo Microsoft Edge para acceder a sus preferencias de navegación y favoritos. Para obtener más información, vea Install and configure the new Microsoft Edge.
- Una vez que hayas iniciado sesión Surface Hub, puedes usar otras aplicaciones sin tener que volver a iniciar sesión hasta que **selecciones Finalizar sesión**. Al seleccionar **Finalizar sesión,** se eliminan las credenciales, los archivos y los datos personales del dispositivo. Para obtener más información, vea End session.

Obtén más información

- Opciones de autenticación sin contraseña para Azure Active Directory
- Inicio de sesión sin contraseña con la Microsoft Authenticator aplicación
- Inicio de sesión sin contraseña con claves de seguridad FIDO2

Cómo gestiona Surface Hub los problemas de seguridad de Wi-Fi Direct

12/01/2022 • 13 minutes to read

Microsoft Surface Hub es un dispositivo de productividad todo en uno que permite a los equipos realizar una mejor lluvia de ideas, colaborar y compartir ideas. Surface Hub depende de Miracast para la proyección inalámbrica a través de Wi-Fi Direct.

En este artículo se describen las vulnerabilidades de seguridad de Wi-Fi Direct, cómo afronta Surface Hub esos riesgos y cómo los administradores pueden configurar Surface hub para obtener el mayor nivel de seguridad. Esta información ayudará a los clientes que tienen requisitos de alta seguridad a proteger sus redes conectadas en el Hub y los datos en tránsito.

Las audiencias previstas para este artículo son administradores de ti y de redes que desean implementar Surface Hub en su entorno corporativo con una configuración de seguridad óptima.

Introducción

La seguridad de Surface Hub depende ampliamente de Wi-Fi Direct/Miracast y de los estándares asociados de 802,11, Wi-Fi Protected Access (WPA2) y de configuración protegida inalámbrica (WPS). Dado que el dispositivo solo es compatible con WPS (a diferencia de la clave previamente compartida de WPA2 o WPA2 Enterprise), los problemas que se suelen asociar con el cifrado de 802,11 se simplifican.

Surface Hub funciona de su equivalente con el campo de los receptores Miracast. Por lo tanto, es vulnerable a un conjunto similar de exploits que todos los dispositivos de red inalámbrica basados en WPS. Pero la implementación de Surface Hub de WPS tiene precauciones adicionales integradas. Además, su arquitectura interna ayuda a evitar que un atacante que ha puesto en peligro la capa Wi-Fi Direct o Miracast pase la interfaz de red a otras superficies de ataque y redes empresariales conectadas.

Wi-Fi Direct en segundo plano

Miracast forma parte del estándar de visualización de Wi-Fi, que es compatible con el protocolo Wi-Fi Direct. Estos estándares son compatibles con dispositivos móviles modernos para colaboración y uso compartido de pantalla.

Wi-Fi Direct o Wi-Fi "de par a par" (P2P) es un estándar de la Alianza Wi-Fi para redes "ad-hoc". Los dispositivos compatibles pueden comunicarse directamente y crear grupos de redes sin un punto de acceso o conexión a Internet convencional.

WPA2 proporciona seguridad para Wi-Fi Direct en el estándar WPS. El mecanismo de autenticación para dispositivos puede ser un PIN numérico (código PIN de WPS), un botón de inserción físico o virtual (WPS-PBC) o un mensaje fuera de banda, como una comunicación Near Field (WPS-OOO). Surface Hub admite el método de ANCLAr y el método pulsador, que es el predeterminado.

En Wi-Fi Direct, los grupos se crean como uno de los siguientes tipos:

- *Persistente*, en el que puede realizarse la reconexión automática mediante material de clave almacenado
- *Temporal*, en el que los dispositivos no pueden volver a autenticarse sin la acción del usuario

Los grupos de Wi-Fi Direct determinan el propietario de un *Grupo* (ir) a través de un protocolo de negociación, que imita la funcionalidad "estación" o "punto de acceso" para el grupo de Wi-Fi Direct establecido. Wi-Fi Direct

GO proporciona autenticación (a través de un "registrador interno") y facilita la transmisión de conexiones de red. Para Surface Hub, la negociación de este GO no se produce. La red solo funciona en modo "autónomo" y Surface Hub siempre es el propietario del grupo. Por último, Surface Hub no se une a otras redes Wi-Fi Direct como cliente.

Cómo afronta Surface Hub las vulnerabilidades de Wi-Fi Direct

Vulnerabilidades y ataques en las invitaciones directas, la difusión y el proceso de detección de Wi-Fi: Los ataques de Wi-Fi Direct/Miracast pueden dirigirse a debilidades en el establecimiento de grupos, detección de elementos de mismo nivel, difusión de dispositivo o procesos de invitación.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
El proceso de descubrimiento puede permanecer activo durante un período de tiempo prolongado, lo que puede permitir que se establezcan invitaciones y conexiones sin la aprobación del propietario del dispositivo.	Surface Hub solo funciona como propietario del grupo, que no realiza los procesos de negociación o descubrimiento de clientes. Puede desactivar completamente la proyección inalámbrica para desactivar la difusión.
Invitación y descubrimiento a través de PBC permite que un atacante no autenticado realice repetidos intentos de conexión o se acepten conexiones no autenticadas de forma automática.	Al requerir la seguridad del PIN de WPS, los administradores pueden reducir el potencial de conexiones no autorizadas o "bombas de invitación" en las que las invitaciones se envían repetidamente hasta que un usuario acepta por error.

Botón de comando de configuración de Wi-Fi Protected Setup (WPS) Connect (PBC) vs: Se han demostrado puntos débiles públicos en el diseño y la implementación de métodos de WPS-PIN. WPS-PBC tiene otras vulnerabilidades que podrían permitir ataques activos contra un protocolo diseñado para un uso único.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
WPS-PBC es vulnerable a atacantes activos. La especificación de WPS dice: "el método PBC tiene cero bits de entropía y solo protege contra ataques de escucha pasiva. PBC protege contra los ataques de interceptación y toma medidas para evitar que un dispositivo se una a una red que no seleccionó el propietario del dispositivo. Sin embargo, la ausencia de autenticación significa que PBC no protege contra un ataque activo. " Los atacantes pueden usar una interconexión inalámbrica selectiva o cualquier otra técnica de denegación de servicio para desencadenar una conexión o un conexión Wi-Fi Direct o no deseada. Además, un atacante activo que simplemente tiene la proximidad física puede destruir varias veces cualquier grupo de Wi-Fi Direct e intentar el ataque hasta que se complete.	Habilitar la seguridad de PIN de WPS en la configuración de Surface Hub. La especificación WPS de Wi-Fi dice: "el método PBC solo se debe usar si no hay registrador con capacidad para PIN y el usuario de WLAN está dispuesto a aceptar los riesgos asociados con PBC".
Las implementaciones de PIN de WPS pueden estar sujetas a ataques de fuerza bruta que se destinan a una vulnerabilidad en el estándar de WPS. El diseño de la verificación de PATILLAs dividida condujo varias vulnerabilidades de implementación durante los últimos años en una variedad de fabricantes de hardware de Wi-Fi. En 2011, los investigadores Martín Viehböck y Craig Heffner publicaron información sobre esta vulnerabilidad y herramientas como "Reaver" como prueba de concepto.	La implementación de Microsoft de WPS en Surface Hub cambia el PIN cada 30 segundos. Para descifrar el PIN, un atacante debe completar todo el exploit en menos de 30 segundos. Dado el estado actual de las herramientas y la investigación en esta área, es poco probable que un ataque de craqueo a PIN de fuerza bruta a través de WPS tenga éxito.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
WPS-PIN se puede adivinar mediante un ataque sin conexión debido a una clave inicial débil (E-S1, E S2) entropía. En 2014, Dominique Bongard describía un ataque de "polvo Pixie" en el que la aleatoriedad inicial del generador de números pseudoaleatorios (PRNG) en el dispositivo inalámbrico permitía un ataque de fuerza bruta sin conexión.	La implementación de Microsoft de WPS en Surface Hub no es susceptible a este ataque de la fuerza bruta sin conexión. El PIN de WPS es aleatorio para cada conexión.

Exposición no deseada de servicios de red: Los daemons de red pensados para los servicios de Ethernet o WLAN pueden exponerse accidentalmente debido a un error de configuración (como el enlace a interfaces "todas"/0.0.0.0). Otras causas posibles son que el firewall del dispositivo esté mal configurado o que falten reglas de Firewall.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Un error de configuración enlaza un servicio de red no autenticado o vulnerable a interfaces "all", incluida la interfaz de Wi-Fi Direct. Esto puede exponer servicios que no deberían ser accesibles para clientes de Wi-Fi Direct, que pueden autenticarse de manera débil o automática.	En Surface Hub, las reglas de Firewall predeterminadas solo permiten los puertos de red TCP y UDP requeridos y deniegan de forma predeterminada todas las conexiones entrantes. Habilite el modo de PIN de WPS para configurar la autenticación robusta.

Puentes de Wi-Fi Direct y otras redes cableadas o inalámbricas: El puente de red entre redes WLAN o Ethernet es una violación de la especificación Wi-Fi Direct. Un puente o una configuración no recomendable puede reducir o quitar de forma eficaz los controles de acceso inalámbrico para la red corporativa interna.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Los dispositivos de Wi-Fi Direct podrían permitir acceso no autenticado o deficiente para las conexiones de red conectadas. Esto podría permitir que las redes Wi-Fi Direct enruten el tráfico a una LAN Ethernet interna u otra infraestructura o a redes WLAN de la empresa infringiendo los protocolos de seguridad de TI existentes.	Surface Hub no se puede configurar para enlazar interfaces inalámbricas o permitir el enrutamiento entre redes dispares. Las reglas de firewall predeterminadas agregan una defensa más profunda para este tipo de conexiones de enrutamiento o puente.

El uso del modo Wi-Fi Direct "heredado": La exposición a redes o dispositivos no deseados puede producirse cuando opera en modo "heredado". Si no está habilitado el PIN de WPS, se podrían producir conexiones no intencionadas o suplantación de identidades del dispositivo.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Al ser compatible con los clientes de infraestructura 802.11 y Wi-Fi Direct, el sistema funciona en un modo de compatibilidad "heredado". Esto puede exponer la fase de configuración de la conexión de forma indefinida, lo que permite que los grupos se unan o los dispositivos invitados a conectarse correctamente después de finalizar la fase de configuración previstas.	Surface Hub no es compatible con clientes heredados de Wi-Fi Direct. Solo se pueden realizar conexiones de Wi-Fi Direct a Surface Hub, incluso cuando el modo PIN de WPS está habilitado.

Negociación de Wi-Fi Direct go durante la configuración de la conexión: El propietario del grupo en Wi-Fi Direct es análogo al "punto de acceso" en una red inalámbrica de 802,11 convencionales. Un dispositivo malintencionado puede sortear la negociación.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Si se establecen dinámicamente grupos o se puede hacer que el dispositivo Wi-Fi Direct se unan a grupos nuevos, la negociación de propietarios del grupo puede hacerse con un dispositivo malintencionado que siempre especifica el valor máximo de 15 como propietario del grupo. (Pero se produce un error en la conexión si el dispositivo está configurado para ser siempre un propietario del grupo).	Surface Hub aprovecha el modo autónomo "Wi-Fi Direct", que omite la fase de negociación GO de configuración de conexión. Y Surface Hub siempre es el propietario del grupo.

Desautenticación de Wi-Fi inesperada o malintencionada: La desautenticación Wi-Fi es un ataque antiguo en el que un atacante local puede acelerar la pérdida de información en el proceso de configuración de la conexión, desencadenar nuevos protocolos de enlace de cuatro vías, dirigirse a una versión de Wi-Fi Direct-PBC para ataques activos o crear ataques de denegación de servicio.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Los atacantes no autenticados pueden enviar paquetes de deautenticación para hacer que la estación se vuelva a autenticar y rastrear el protocolo de enlace resultante. Pueden intentarse ataque criptográfico o de fuerza bruta en el protocolo de enlace resultante. La mitigación de estos ataques incluye la aplicación de directivas de longitud y complejidad para las claves previamente compartidas, la configuración del punto de acceso (si procede) para detectar niveles malintencionados de paquetes de desautenticación y el uso de WPS para generar automáticamente claves seguras. En el modo PBC, el usuario interactúa con un botón físico o virtual para permitir una asociación de dispositivo arbitraria. Este proceso solo debe realizarse durante la configuración, en un breve lapso de tiempo. Después de insertar el botón automáticamente, el dispositivo aceptará cualquier estación que se asocie a un valor de PIN canónico (todos los ceros). La desautenticación puede forzar un proceso de instalación repetido.	Surface Hub usa WPS en modo PIN o PBC. No se permite ninguna configuración de PSK. Este método ayuda a exigir la generación de claves sólidas. Lo mejor es habilitar la seguridad de PIN de WPS para Surface Hub.
Además de los ataques de denegación de servicio, los paquetes de desautenticación se pueden usar para desencadenar una reconexión que vuelva a abrir la ventana de oportunidad de ataques activos contra WPS-PBC.	Habilitar la seguridad de PIN de WPS en la configuración de Surface Hub.

Revelación de información inalámbrica básica: Las redes inalámbricas, 802,11 o de otro modo, son inherentes al riesgo de revelación de información. Aunque esta información es principalmente metadatos de conexión o dispositivo, este problema sigue siendo un riesgo conocido para cualquier administrador de red de 802,11. Wi-Fi Direct con autenticación de dispositivos a través de PIN de WPS revela eficazmente la misma información como una red PSK o Enterprise 802.11

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Durante la difusión, la configuración de la conexión o incluso el funcionamiento normal de las conexiones ya cifradas, la información básica sobre los dispositivos y los tamaños de los paquetes es transmitida de manera inalámbrica. En un nivel básico, un atacante local que se encuentra dentro del rango inalámbrico puede examinar los elementos de información de 802,11 pertinentes para determinar los nombres de los dispositivos inalámbricos, las direcciones MAC de los equipos de comunicación y posiblemente otros detalles, como la versión de la pila inalámbrica, los tamaños de paquete o las opciones del punto de acceso configurado o el propietario del grupo.	La red Wi-Fi Direct que usa Surface Hub no puede protegerse aún más de las pérdidas de metadatos, como las de 802,11 Enterprise o PSK Wireless. La seguridad física y la eliminación de las amenazas potenciales de la proximidad inalámbrica pueden ayudar a reducir las fugas potenciales en información.

Ataques inalámbricos de gemelas o de suplantación: La suplantación de nombre inalámbrico es un ataque sencillo y muy conocido que puede usar un atacante local para atraer a usuarios insospechados o malintencionados para que se conecten.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Al imitar o clonar el nombre inalámbrico o el "SSID" de la red de destino, un atacante puede engañar al usuario para que se conecte a una red falsa y malintencionada. Al permitir la combinación automática de Miracast sin autenticar, un atacante podría capturar los materiales de visualización previstos o lanzar ataques de red en el dispositivo de conexión.	Aunque no existen protecciones específicas contra la Unión a un Surface Hub imitado, esta vulnerabilidad se ha mitigado parcialmente de dos maneras. En primer lugar, cualquier potencial ataque debe producirse físicamente dentro del alcance Wi-Fi. En segundo lugar, este ataque solo es posible durante la primera conexión. Las conexiones posteriores usan un grupo de Wi-Fi Direct persistente y Windows recordará y establecerá la prioridad de esta conexión anterior durante el uso del concentrador. (Nota: no se consideró la suplantación de la dirección MAC, el canal Wi-Fi y el SSID al mismo tiempo para este informe y esto puede dar lugar a un comportamiento de Wi-Fi incoherente). En general, este punto débil es un problema fundamental para cualquier red inalámbrica de 802,11 que carezca de protocolos de WPA2 empresarial como EAP-TLS o EAP-PWD, que no es compatible con Wi-Fi Direct.

Directrices de refuerzo de Surface Hub

Surface Hub está diseñado para facilitar la colaboración y permitir que los usuarios puedan iniciar o unirse a reuniones de una manera rápida y eficaz. La configuración predeterminada de Wi-Fi Direct para Surface Hub está optimizada para este escenario.

Para la seguridad de interfaz inalámbrica adicional, los usuarios de Surface Hub deben habilitar la configuración de seguridad de WPS-PIN. Esta opción deshabilita el modo WPS-PBC y ofrece autenticación de cliente. Proporciona el nivel de protección más potente evitando la conexión no autorizada a Surface Hub.

Si aún tienes dudas sobre la autenticación y la autorización de Surface Hub, te recomendamos que conectes el dispositivo a una red independiente. Puede usar Wi-Fi (como una red Wi-Fi "de invitado") o una red Ethernet independiente, preferiblemente una red física totalmente diferente. Pero una VLAN también puede proporcionar seguridad adicional. Por supuesto, este enfoque puede impedir las conexiones a los recursos o servicios de la red interna y puede requerir una configuración de red adicional para recuperar el acceso.

También se recomienda:

- Instalar actualizaciones normales del sistema
- Actualizar la configuración de Miracast para deshabilitar el modo de presentación automática

Más información

- Especificaciones de Wi-Fi Direct
- Especificación de Wireless Protected Setup (WPS)

Historial de actualizaciones de SurfaceHub

12/01/2022 • 30 minutes to read

Windows 10 diseñado para ser un servicio, lo que significa que mejora automáticamente a través de actualizaciones periódicas de software. La gran noticia es que normalmente no tiene que hacer nada para obtener las últimas actualizaciones de Windows 10, que se descargarán e instalarán siempre que estén disponibles.

La mayoría Windows actualizaciones se centran en mejoras de rendimiento y seguridad para mantenerte en funcionamiento las 24 horas del día, los 7 días de la noche.

Una cosa que escuchamos de usted es que desea saber más sobre lo que hay en nuestras actualizaciones de Windows 10, por lo que proporcionamos más detalles en esta página. En la lista siguiente, primero se muestra la actualización Windows actualización con Surface Hub mejoras específicas de la aplicación. Las actualizaciones son acumulativas, por lo que la instalación de la última actualización Windows disponible (incluso si no está en la lista siguiente) garantiza que también se beneficie de las mejoras en las actualizaciones anteriores. Microsoft Store las aplicaciones se actualizan a través del Microsoft Store (administrado por el administrador del Surface Hub del usuario). Los detalles sobre las actualizaciones de aplicaciones se proporcionan por aplicación.

Actualizaremos esta página a medida que se den a conocer nuevas actualizaciones, así que mantente al tanto de la información más reciente. Y gracias por ayudarnos a aprender y mejorar con cada actualización.

Consulte la página "Surface Hub Informaciónimportante " para temas relacionados sobre las versiones actuales y pasadas que puedan requerir su atención.

Windows 10 Team 2020 Update (20H2)

▶ 30 de septiembre de 2021: KB5004196, KB5004198 y KB5004199
▶ 30 de septiembre de 2021: actualización para Team basada en KB5005611* (compilación del sistema operativo 19042.1266)
▶ 1 de septiembre de 2021: actualización para Team basada en KB5005101* (compilación del sistema operativo 19042.1202)
▶ 29 de julio de 2021: actualización para Team basada en KB5004296* (compilación del sistema operativo 19042.1151)
▶ 10 de junio de 2021: actualización para Surface Hub 2S
▶ 13 de abril de 2021: actualización para Team basada en KB5001330* (compilación del sistema operativo 19042.928)
▶ 13 de marzo de 2021: actualización para Surface Hub 2S
▶ 2 de febrero de 2021: actualización para Team basada en KB4598291* (compilación del sistema operativo 19042.789)
▶ 15 de enero de 2021: actualización para Surface Hub 2S
▶ 11 de diciembre de 2020: actualización para Surface Hub 2S
▶ 30 de noviembre de 2020: actualización para Team basada en KB4586853* (compilación del sistema operativo 19042.662)
▶ 24 de noviembre de 2020: actualización para Surface Hub 2S
▶ 27 de octubre de 2020: actualización para Surface Hub 2S
▶ Windows 10 Team 2020 Update for Surface Hub— Notas de la versión general (compilación del sistema operativo 19042.572)

Windows 10 Team Actualización de creadores (1703)

▶ 1 de septiembre de 2020: actualización para Surface Hub 2S
▶ 4 de mayo de 2020: actualización para Surface Hub 2S
▶ 28 de febrero de 2020: actualización para Surface Hub 2S
▶ 11 de febrero de 2020: actualización para Team basada en KB4537765* (compilación del sistema operativo 15063.2284)
▶ 14 de enero de 2020: actualización para team basada en KB4534296* (compilación del sistema operativo 15063.2254)
▶ 24 de septiembre de 2019: actualización para Team basada en KB4516059* (compilación del sistema operativo 15063.2078)
▶ 17 de agosto de 2019: actualización para Team basada en KB4512474* (compilación del sistema operativo 15063.2021)
▶ 18 de junio de 2019: actualización para Team basada en KB4503289* (compilación del sistema operativo 15063.1897)
▶ 28 de mayo de 2019: actualización para Team basada en KB4499162* (compilación del sistema operativo 15063.1835)
▶ 25 de abril de 2019: actualización para Team basada en KB4493436* (compilación del sistema operativo 15063.1784)
▶ 27 de noviembre de 2018: actualización para Team basada en KB4467699* (compilación del sistema operativo 15063.1478)
▶ 18 de octubre de 2018: actualización para Team basada en KB4462939* (compilación del sistema operativo 15063.1418)
▶ 31 de agosto de 2018: actualización para Team basada en KB4343889* (compilación del sistema operativo 15063.1292)
▶ 21 de junio de 2018: actualización para Team basada en KB4284830* (compilación del sistema operativo 15063.1182)
▶ 17 de abril de 2018: actualización para Team basada en KB4093117* (compilación del sistema operativo 15063.1058)
▶ 23 de febrero de 2018: actualización para team basada en KB4077528* (compilación del sistema operativo 15063.907)
▶ 16 de enero de 2018: actualización para Team basada en KB4057144* (compilación del sistema operativo 15063.877)
▶ 12 de diciembre de 2017: actualización para Team basada en KB4053580* (compilación del sistema operativo 15063.786)
▶ 14 de noviembre de 2017: actualización para Team basada en KB4048954* (compilación del sistema operativo 15063.726)
▶ 10 de octubre de 2017: actualización para team basada en KB4041676* (compilación del sistema operativo 15063.674)
▶ 12 de septiembre de 2017: actualización para Team basada en KB4038788* (compilación del sistema operativo 15063.605)
▶ 1 de agosto de 2017: actualización para Team basada en KB4032188* (compilación del sistema operativo 15063.498)
▶ 27 de junio de 2017: actualización para Team basada en KB4022716* (compilación del sistema operativo 15063.442)
▶ 13 de junio de 2017: actualización para team basada en KB4022725* (compilación del sistema operativo 15063.413)
▶ 24 de mayo de 2017: actualización para Team basada en KB4021573* (compilación del sistema operativo 15063.328)
▶ 9 de mayo de 2017: actualización para Team basada en KB4016871* (compilación del sistema operativo 15063.296)
▶ Windows 10 Team Creators Update 1703 for Surface Hub— Notas de la versión general (compilación del sistema operativo 15063.0)

Windows 10 Team Actualización de aniversario (1607)

▶ 14 de marzo de 2017: actualización para Team basada en KB4013429* (compilación del sistema operativo 14393.953)
▶ 10 de enero de 2017: actualización para team basada en KB4000825* (compilación del sistema operativo 14393.693)
▶ 13 de diciembre de 2016: actualización para Team basada en KB3206632* (compilación del sistema operativo 14393.576)
▶ 4 de noviembre de 2016: actualización para Team basada en KB3200970* (compilación del sistema operativo 14393.447)
▶ 25 de octubre de 2016: actualización para Team basada en KB3197954* (compilación del sistema operativo 14393.351)
▶ 11 de octubre de 2016: actualización para Team basada en KB3194496* (compilación del sistema operativo 14393.222)

Actualizaciones para Windows 10 versión 1511

▶ 4 de noviembre de 2016: actualización para Team basada en KB3198586* (compilación del sistema operativo 10586.679)
▶ 12 de julio de 2016: actualización para Team basada en KB3172985* (compilación del sistema operativo 10586.494)
▶ 14 de junio de 2016: actualización para Team basada en KB3163018* (compilación del sistema operativo 10586.420)
▶ 10 de mayo de 2016: actualización para Team basada en KB3156421* (compilación del sistema operativo 10586.318)
▶ 12 de abril de 2016: actualización para Team basada en KB3147458* (compilación del sistema operativo 10586.218)

Temas relacionados

- Información de versión de Windows 10
- Windows 10 Actualización de noviembre: Preguntas frecuentes
- Historial de actualizaciones de Microsoft Surface
- Historial de actualizaciones de Microsoft Lumia
- Obtén Windows 10

Restablecer y recuperar para Surface Hub 2S

12/01/2022 • 3 minutes to read

Si tienes problemas con Surface Hub 2S, puedes restablecer el dispositivo a la configuración de fábrica o restaurarlo mediante una unidad USB.

Para empezar, inicie sesión en Surface Hub 2S con credenciales de administrador, abra la aplicación **Configuración,** seleccione Actualizar **& seguridad**y, a continuación, seleccione **Recuperación**.

Restablecer el dispositivo

> **IMPORTANT**
>
> Asegúrate de que tienes la clave de BitLocker disponible antes de restablecer el dispositivo, como se te pedirá más adelante. Para obtener más información, consulta Guardar la clave de BitLocker.

1. Para restablecer el dispositivo, **selecciona Introducción**.
2. Cuando aparezca **la ventana Listo para restablecer** este dispositivo, seleccione **Restablecer**.

   > **TIP**
   >
   > Cuando el concentrador se reinicia en la partición de recuperación, se te pedirá que escribas la clave de BitLocker. Si se omite ese mensaje, se producirá un error en el restablecimiento. Una vez que escribes la clave de BitLocker, el concentrador vuelve a instalar el sistema operativo desde la partición de recuperación. Esto puede tardar hasta una hora en completarse.

3. Para volver a configurar el dispositivo, ejecute el programa de instalación por primera vez.
4. Si administras el dispositivo con Microsoft Intune u otra solución de administración de dispositivos móviles, retira y elimina el registro anterior y, a continuación, vuelve a inscribir el nuevo dispositivo. Para obtener más información, consulta Quitar dispositivos con borrar, retirar o desenrollar manualmente el dispositivo.

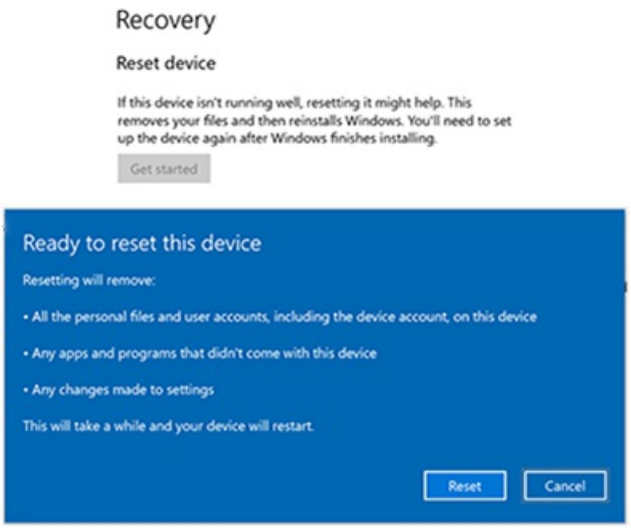


Figura 1. Restablecer y recuperar para Surface Hub 2S

Recuperar Surface Hub 2S mediante una unidad de recuperación USB

Como novedad Surface Hub 2S, ahora puedes reinstalar el dispositivo mediante una imagen de recuperación.

Recuperación desde una unidad USB

Con Surface Hub 2S, puedes reinstalar el dispositivo mediante una imagen de recuperación. Al hacerlo, puedes reinstalar el dispositivo en la configuración de fábrica si has perdido la clave de BitLocker o si ya no tienes credenciales de administrador en la Configuración aplicación.

> **TIP**
> Usa una unidad USB 3.0 con 8 GB o 16 GB de almacenamiento, con el formato FAT32.

1. Desde un equipo independiente, descarga la .zip de recuperación de archivos desde el sitio web de Recuperación de Surface y, a continuación, vuelve a estas instrucciones.
2. En el cuadro de búsqueda de la barra de tareas, **escriba**unidad de recuperación y, a continuación, seleccione Crear una unidad de recuperación o Unidad **de** recuperación **a** partir de los resultados. Es posible que deba escribir una contraseña de administrador o confirmar su elección.
3. En el **cuadro Control de cuentas de** usuario, seleccione **Sí**.
4. Asegúrese de borrar la casilla Copia de seguridad de **archivos del sistema en la unidad** de recuperación y, a continuación, seleccione **Siguiente**.
5. Seleccione la unidad USB y, a continuación, **seleccione Siguiente > Crear**. Algunas utilidades deben copiarse en la unidad de recuperación, por lo que esto puede tardar unos minutos.
6. Cuando la unidad de recuperación esté lista, seleccione **Finalizar**.
7. Haga doble clic en la imagen de .zip archivo que descargó anteriormente para abrirlo.
8. Seleccione todos los archivos de la carpeta de imagen de recuperación, cópielos en la raíz de la unidad USB y, a continuación, seleccione Elegir para reemplazar los **archivos en el destino**.
9. Una vez que los archivos han terminado de copiarse, selecciona el icono **Quitar hardware** y medios de expulsar de forma segura en la barra de tareas y quita la unidad USB.
10. Conectar la unidad USB a cualquier puerto USB-C o USB-A del Surface Hub 2S. Desactiva el concentrador y, a continuación, arranca desde la unidad USB.

Arranque Surface Hub desde una unidad USB

> **NOTE**
> Si el dispositivo se desenchufó o experimentó un corte de energía de abrubt o un cable de alimentación, espere al menos 15 segundos antes de intentar arrancar desde USB.

1. Al presionar el botón Bajar volumen, presione el botón De encendido.
2. Sigue presionando ambos botones hasta que veas el Windows logotipo.
3. Suelta el botón De encendido pero mantén presionado el botón Bajar volumen hasta que comience la instalación de la interfaz de usuario.

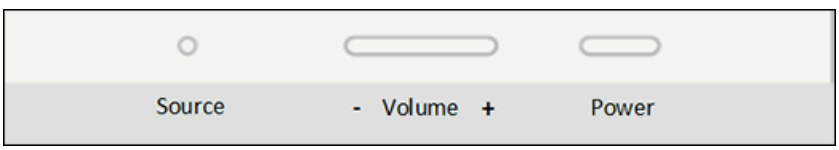


Figura 2. Botones de volumen y encendido

4. En la pantalla de selección de idioma, seleccione el idioma de presentación para su Surface Hub 2S.
5. Seleccione **Recuperar de una unidad y** Limpiar completamente **la**unidad y, a continuación, seleccione **Recuperar**. Si se te pide una clave de BitLocker, selecciona **Omitir esta unidad**. Surface Hub 2S se reinicia varias veces y puede tardar una hora o más en completar el proceso de recuperación.
6. Cuando aparezca la pantalla de configuración por primera vez, quite la unidad USB.

Contactar con el soporte técnico

Si tiene preguntas o necesita ayuda, puede crear una solicitud de soporte técnico.

Soluciona problemas de Miracast en Surface Hub

12/01/2022 • 6 minutes to read

Surface Hub admite la proyección inalámbrica a través del protocolo Miracast. La mayoría de los monitores y adaptadores inalámbricos disponibles hoy en día usan la implementación original de Miracast. Surface Hub usa una versión de Miracast ligeramente diferente conocida como **Miracast Autonomous Group Owner (AGO)**. Un paso común de solución de problemas cuando se produce un error en la proyección inalámbrica a Surface Hub es probar a proyectar a otro monitor o adaptador inalámbrico. Sin embargo, en la mayoría de los casos, estos dispositivos no usan Miracast AGO y no gestiona la proyección inalámbrica del mismo modo que lo hace Surface Hub.

En el Miracast tradicional, el dispositivo de proyección conectará el punto de acceso configurado por el monitor habilitado para Miracast y luego el monitor enviará el tráfico al dispositivo de proyección mediante el canal de red del este último. Miracast AGO es un proceso de conexión de dos pasos:

- El primer paso es una conexión inicial a 2,4GHz.
- Después de ese protocolo de enlace inicial, el dispositivo de proyección envía el tráfico al monitor con la configuración de canal inalámbrico de este. Si Surface Hub está conectado a una red Wi-Fi, el punto de acceso, usará el mismo canal que la red conectada, de lo contrario usará el canal de Miracast que se indica en la configuración.

Por lo general, hay dos tipos de problemas con Miracast a Surface Hub: conexión y rendimiento. En cualquier caso, es una buena idea obtener una imagen general de la actividad de la red inalámbrica en la ubicación del Surface Hub. Si ejecutas una herramienta de análisis de red, verás las redes disponibles y el uso de canal del entorno.

Problemas de conexión

Asegúrate de que Wi-Fi y Miracast están habilitados en la configuración de Surface Hub.

Si ejecutaste un análisis de red, deberías ver Surface Hub Miracast en la lista de puntos de acceso. Si la red Miracast de Surface Hub se muestra en el análisis, pero no puede verla como un dispositivo disponible, puede intentar ajustar el canal Miracast usado por Surface Hub.

Cuando Surface Hub está conectado a una red Wi-Fi, usará la misma configuración de canal que el punto de acceso Wi-Fi para su punto de acceso de Miracast. Para solucionar problemas, desconecta Surface Hub desde las redes Wi-Fi (pero mantén Wi-Fi habilitado), para que puedas controlar el canal que se usa para Miracast. Puedes seleccionar manualmente el canal de Miracast en Configuración. Tendrás que reiniciar el Surface Hub después de cada cambio. Por lo general, es recomendable usar los canales que no muestran un uso intensivo tras el análisis de la red.

También es posible que el problema de conexión sea el resultado de un problema en el dispositivo de conexión. Si el dispositivo de proyección ejecuta Windows, debería ser Windows 8.1 o una versión posterior para asegurar compatibilidad completa con Miracast. Nuevamente, para la solución de problemas, desconecta el dispositivo de proyección de las redes Wi-Fi. De este modo, se eliminará cualquier cambio de canal entre el canal de punto de acceso y el canal de Miracast establecido en Surface Hub. Asimismo, es posible que algunas opciones de configuración de directiva de grupo y del firewall estén asociadas a una red Wi-Fi.

Comprobar controladores

También es recomendable asegurarte de que los controladores y las actualizaciones más recientes estén instalados en el dispositivo de proyección. En el Administrador de dispositivos, abre el adaptador Wi-Fi y

adaptador de vídeo, y comprueba si hay una versión de controlador actualizada. Es recomendable instalar la revisión 3120232 para Surface Pro 3 y Surface Pro 4 si estos dispositivos usan un controlador Wi-Fi más antiguo.

Comprobar la compatibilidad de Miracast

A continuación, asegúrate de que Miracast se admite en el dispositivo.

1. Presiona la tecla Windows + R y escribe `dxdiag`.
2. Haga clic en "guardar toda la información".
3. Abre el archivo dxdiag.txt guardado y busca **Miracast**. Debe aparecer **Available, with HDCP**.

Comprobar el firewall

El firewall de Windows puede bloquear el tráfico de Miracast. La prueba más sencilla consiste en deshabilitar el firewall y probar la proyección. Si Miracast funciona con el firewall deshabilitado, agrega una excepción.

```
C:\Windows\System32\WUDFHost.exe
Allow In/Out connections for TCP and UDP, Ports: All.
```

Comprobar la configuración de directiva de grupo

En los dispositivos unidos a un dominio, la directiva de grupo también puede bloquear Miracast.

1. Usa la tecla Windows + R y escribe `rsop.msc` para ejecutar el complemento **Conjunto resultante de directivas**. De este modo, se mostrarán las directivas actuales que se aplican al equipo.
2. Consulta la información de **Configuración del equipo** > **Configuración de Windows** > **Configuración de seguridad** > **Directivas de red inalámbrica (IEEE 802.11)**. Debería haber una opción de configuración para las directivas de conexiones inalámbricas.
3. Haz doble clic en la configuración de las directivas conexiones inalámbricas. Aparecerá un cuadro de diálogo.
4. Abre la pestaña **Permisos de red** y selecciona **Permitir a todos crear perfiles de todos los usuarios**.

Comprobar los registros de eventos

El último lugar donde comprobar es en los registros de eventos. Los eventos de Miracast se registrarán en **Wlanautoconfig**. Esto sucede en Surface Hub y en el dispositivo de proyección. Si exporta los registros de Surface Hub, puede ver los Wlanautoconfig de Surface Hub en la carpeta **WindowsEventLog** . Los errores en el registro de eventos pueden proporcionar algunos detalles adicionales sobre dónde se produce el error de conexión.

Problemas de rendimiento

Cuando se haya conectado una proyección inalámbrica, es posible se produzcan problemas de rendimiento que provocan latencia. Esto suele ser el resultado de una saturación general del canal o de una situación que provoca cambios de canal.

En el caso de saturación del canal, consulta el análisis de red y prueba a usar canales con menos tráfico.

Los cambios de canal se producen cuando el adaptador Wi-Fi necesita enviar tráfico a varios canales. Algunos canales admiten la selección de frecuencia dinámica (DFS). DFS se usa en los canales 49 a 148. Algunos controladores Wi-Fi tendrán un rendimiento deficiente cuando se conectan a un canal DFS. Si experimentas un rendimiento deficiente de Miracast mientras estés conectado a un canal DFS, prueba a realizar la proyección en un canal que no sea DFS. Tanto Surface Hub y como el dispositivo proyección deben usar canales no DFS.

Si Surface Hub y el dispositivo de proyección están conectados a Wi-Fi, pero con distintos puntos de acceso con diferentes canales, Surface Hub y el dispositivo de proyección estará obligado a cambiar de canal mientras está conectado Miracast. Esto resultará en una proyección inalámbrica deficiente y un rendimiento de red deficiente a través de Wi-Fi. Los cambios de canal afectarán al rendimiento de todo el tráfico inalámbrico, no solo la

proyección inalámbrica.

Los cambios de canal también se producirán si el dispositivo de proyección está conectado a una red Wi-Fi con un canal diferente que el canal que Surface Hub usa para Miracast. Por lo tanto, un procedimiento recomendado es establecer el canal Miracast del Surface Hub en el mismo canal que el punto de acceso que se usa con más frecuencia.

Si hay varios puntos de acceso o redes Wi-Fi en el entorno, es inevitable que se produzcan algunos cambios de canal. Para resolver esto, es recomendable que todos los controladores Wi-Fi estén actualizados.

Ponerse en contacto con soporte técnico

Si tiene alguna pregunta o necesita ayuda, puede crear una solicitud de soporte técnico.

Resumen

12/01/2022 • 2 minutes to read

En cumplimiento de las normativas gubernamentales regionales, todos los dispositivos inalámbricos de 5 GHz en Europa, Japón e Israel no admiten la banda U-NII-3. En Surface Hub, los canales asociados con U-NII-3 son de 149 a 165. Esto incluye la conexión Miracast en estos canales. Por lo tanto, Surface Hub que se usan en Europa, Japón e Israel no pueden usar los canales 149 a 165 para conexiones Miracast.

Más información

Para obtener más información, consulte el tema U-NII en Wikipedia.

> **NOTE**
> Microsoft proporciona información de contacto de terceros para ayudarle a encontrar información adicional sobre este tema. Esta información puede cambiar sin previo aviso. Microsoft no garantiza la precisión de la información de terceros.

Surface Hub puede instalar actualizaciones y reiniciar fuera del horario de mantenimiento

12/01/2022 • 2 minutes to read

En determinadas circunstancias, Surface Hub las actualizaciones durante el horario laboral en lugar de durante la ventana de mantenimiento normal. A continuación, el dispositivo se reinicia si es necesario. No puedes usar el dispositivo hasta que se complete el proceso.

> **NOTE**
> Este no es un comportamiento esperado por falta de una ventana de mantenimiento. Solo se produce si el dispositivo está fuera de fecha durante mucho tiempo.

Causa

Para garantizar que Surface Hub esté disponible para su uso durante el horario comercial, el concentrador está configurado para realizar funciones administrativas durante una ventana de mantenimiento que se define en Configuración (vea "Referencias", a continuación). Durante este período de mantenimiento, el concentrador instala automáticamente las actualizaciones disponibles a través de Windows Update o Windows Update for Business (WUfB). Una vez completadas las actualizaciones, el concentrador puede reiniciarse.

Las actualizaciones solo se pueden instalar durante la ventana de mantenimiento si el Surface Hub está activado pero no está en uso o reservado. Por ejemplo, si el Surface Hub está programado para una reunión que dura 24 horas, las actualizaciones programadas para instalarse se aplazarán hasta que el concentrador esté disponible durante la siguiente ventana de mantenimiento. Si el concentrador sigue ocupado y pierde varias ventanas de mantenimiento, el concentrador finalmente empezará a instalar y descargar actualizaciones. Esto puede ocurrir durante o fuera de la ventana de mantenimiento. Una vez iniciada la descarga y la instalación, el dispositivo puede reiniciarse.

Para evitar este problema

Es importante que reserve el tiempo de mantenimiento para Surface Hub realizar funciones administrativas. Reservar el Surface Hub durante intervalos de 24 horas o usar el dispositivo durante la ventana de mantenimiento retrasa la instalación de actualizaciones. Se recomienda no usar ni reservar el concentrador durante el período de mantenimiento programado. Se debe reservar una ventana de dos horas para la actualización.

Una opción que puede usar para controlar la disponibilidad de actualizaciones es Windows Update for Business.

Obtén más información

- Ventana de mantenimiento

Cómo empaquetar y enviar tu Surface Hub 2S para recibir servicio

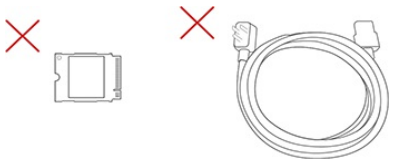
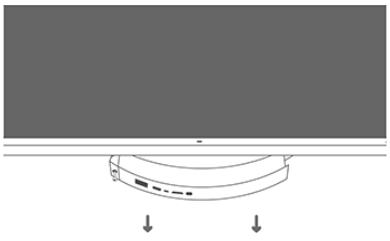
12/01/2022 • 2 minutes to read

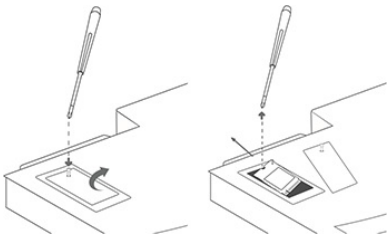
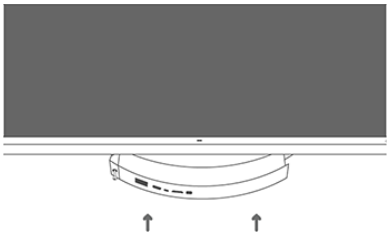
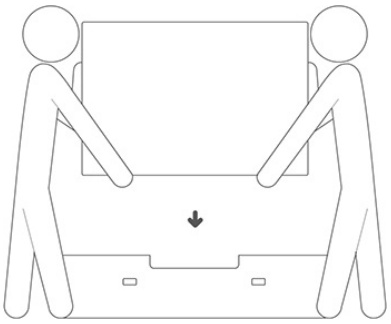
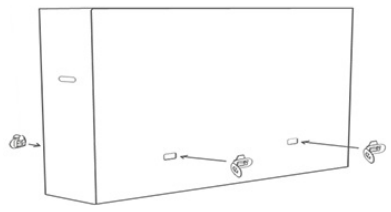
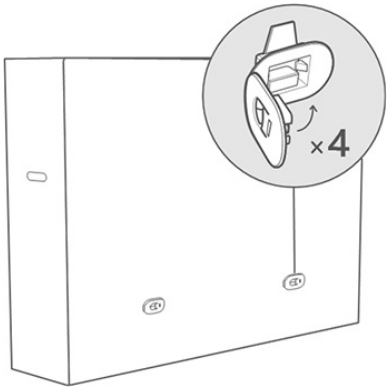
Si reemplazas tu Surface Hub 2S, uno de sus componentes o un accesorio relacionado, usa las instrucciones de este artículo al empaquetar el dispositivo para su envío.

> **IMPORTANT**
> Al empaquetar el dispositivo para el envío, asegúrate de usar el empaquetado en el que llegó el dispositivo de reemplazo.

Cómo empaquetar su Surface Hub 2S 50"

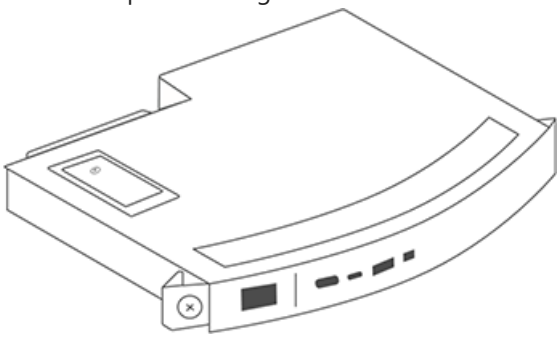
Siga estos pasos para empaquetar su Surface Hub 2S 50" para el envío.

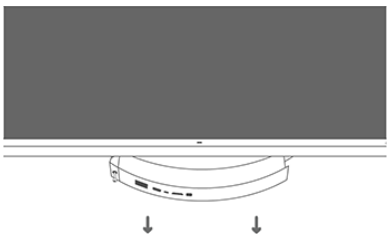
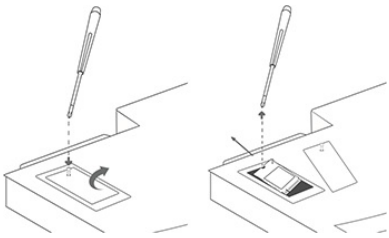
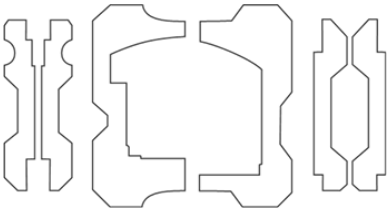
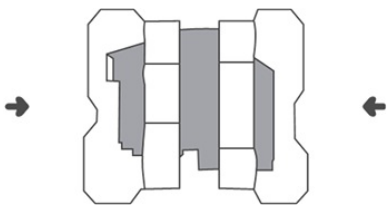
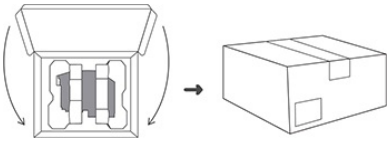
1.	Quite el lápiz y la cámara. No los empaquete con la unidad.	
2.	Quite la unidad y el cable de alimentación. No los empaquete con la unidad. No empaquete la guía de instalación con la unidad.	
3.	Desenchufe todos los cables, deslice la cubierta lateralmente y desenrosque el tornillo de bloqueo del cartucho de cálculo.	
4.	Deslice el cartucho de cálculo fuera de la unidad.	
5.	Necesitará el cartucho de cálculo y un destornillador.	

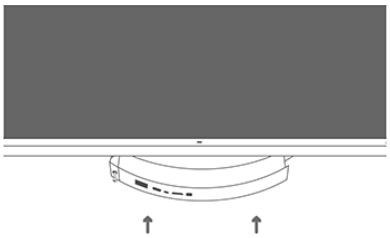
6.	Quite el tornillo de la cubierta y la cubierta del cartucho de cálculo y, a continuación, quite la unidad de estado sólido (SSD).	
7.	Reemplace la cubierta y vuelva a deslizar el cartucho de cálculo en la unidad.	
8.	Vuelva a fijar el tornillo de bloqueo y deslice la cubierta en su lugar.	
9.	Quite cualquier hardware base o de montaje. Con dos personas, coloque la unidad en la base del contenedor de envío.	
10.	Reemplace la cubierta del contenedor de envío e inserte los cuatro clips.	
11.	Cierre los cuatro clips.	

Cómo reemplazar y empaquetar el Surface Hub 2S Compute Cartridge

Siga estos pasos para quitar el Surface Hub 2S Compute Cartridge, empaquetar para su envío e instalar el nuevo compute cartridge.

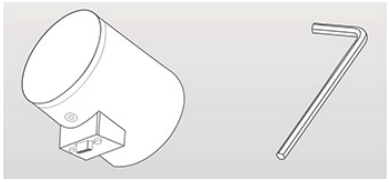
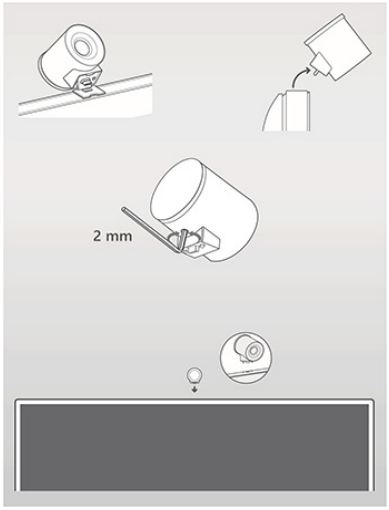


1.	Desenchufe todos los cables, deslice la cubierta lateralmente y desenrosque el tornillo de bloqueo del cartucho de cálculo.	
2.	Deslice el cartucho de cálculo fuera de la unidad.	
3.	Necesitará el cartucho de cálculo y un destornillador.	
4.	Quite el tornillo de la cubierta y la cubierta del cartucho de cálculo y, a continuación, quite la unidad de estado sólido (SSD). Cuando termine, reemplace la cubierta.	
5.	Necesitarás los accesorios de empaquetado que se usaron para empaquetar el paquete de reemplazo de Compute Cartridge.	
6.	Coloque el antiguo cartucho de cálculo en los accesorios de empaquetado.	
7.	Coloque el antiguo cartucho de cálculo y su empaquetado en el cuadro que se usó para el cartucho de cálculo de reemplazo. Vuelva a sesar el cuadro.	

8.	Deslice el cartucho de cálculo de reemplazo en la unidad.	
9.	Fijar el tornillo de bloqueo y deslizar la cubierta en su lugar	

Cómo reemplazar la cámara Surface Hub 2S

Siga estos pasos para quitar la cámara Surface Hub 2S e instalar la nueva cámara.

1.	Necesitarás la nueva cámara y la llave inglesa de dos milímetros.	
2.	Desenchufe la cámara antigua de la unidad. Si es necesario, usa la llave inglesa de Allen para ajustar la nueva cámara. Conecte la nueva cámara a la unidad.	

¿Qué novedades hay en Windows 10, versión 1703 para Microsoft Surface Hub?

12/01/2022 • 2 minutes to read

Mira al ingeniero de Surface Hub, Jordan Marchese, presentar las actualizaciones de Microsoft Surface Hub con Windows 10, versión 1703 (Windows 10 Creators Update).

Windows 10, versión 1703 (también denominada Creators Update), presenta los siguientes cambios para Microsoft Surface Hub.

Nueva configuración

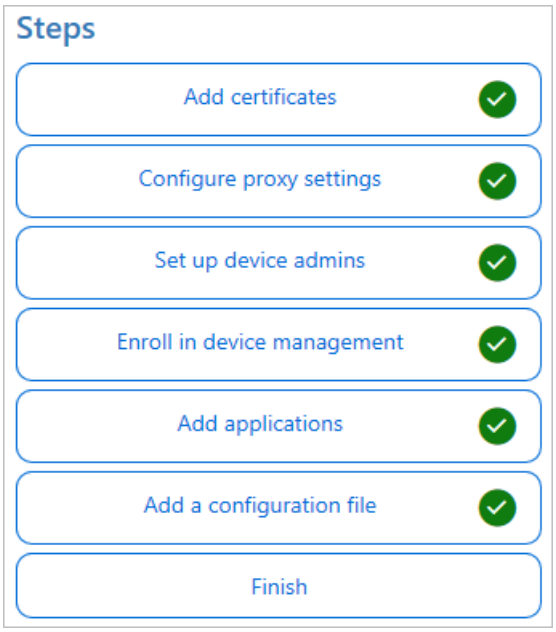
Se ha agregado configuración para la administración de dispositivos móviles (MDM) y los proveedores de servicios de configuración (CSP) para ampliar las capacidades de administración de Surface Hub. La configuración incluye:

- InBoxApps/SkypeForBusiness/DomainName
- InBoxApps/Connect/AutoLaunch
- Properties/DefaultVolume
- Properties/ScreenTimeout
- Properties/SessionTimeout
- Properties/SleepTimeout
- Properties/AllowSessionResume
- Properties/AllowAutoProxyAuth
- Properties/DisableSigninSuggestions
- Properties/DoNotShowMyMeetingsAndFiles
- System/AllowStorageCard

Además de la configuración basada en el nuevo CSP de NetworkQoSPolicy y CSP de NetworkProxy.

Asistente de aprovisionamiento

Un asistente fácil de usar que ayuda a crear rápidamente paquetes de aprovisionamiento que se pueden aplicar a varios dispositivos Surface Hub e incluye la unión en bloque a Azure Active Directory. Obtén información sobre cómo crear un paquete de aprovisionamiento para Surface Hub.



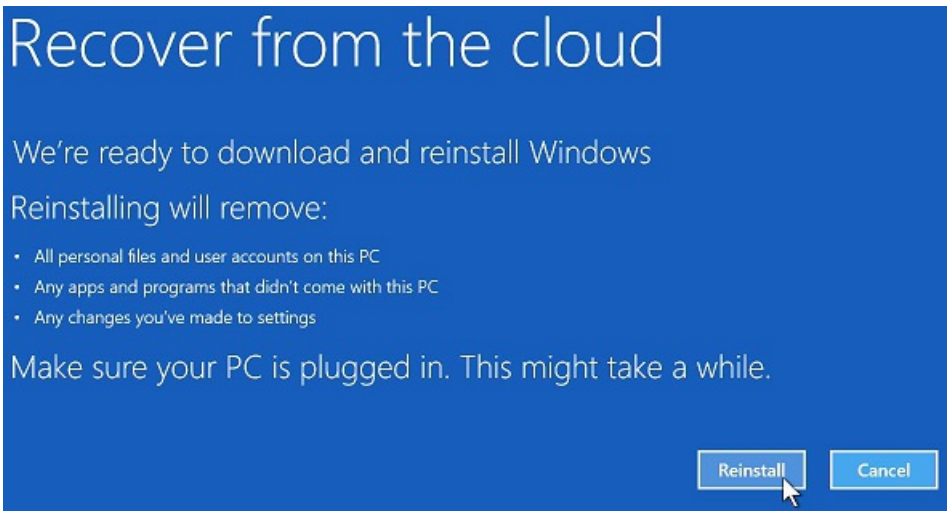
Miracast en la red inalámbrica o LAN existente

Microsoft ha ampliado la capacidad de enviar una emisión de Miracast a través de una red local, en lugar de a través de un vínculo directo inalámbrico.

Recuperación en la nube

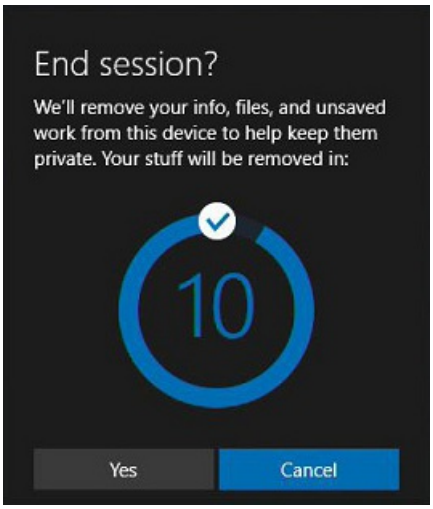
Cuando se restablece un dispositivo Surface Hub, ahora tienes la capacidad de descargar de la nube una compilación de fábrica del sistema operativo e instalarla. Más información sobre la recuperación en la nube.

> **NOTE**
> La recuperación en la nube no funciona si usas servidores proxy.



Finalizar sesión

He terminado es ahora **Finalizar sesión**. Aprende a usar Finalizar sesión.


End session?
We'll remove your info, files, and unsaved work from this device to help keep them private. Your stuff will be removed in:
10
Yes
Cancel

Conceptos básicos del sistema operativo (Surface Hub)

12/01/2022 • 8 minutes to read

El sistema operativo de Surface Hub, Windows 10 Team, se basa en Windows 10 Enterprise y proporciona compatibilidad enriquecida para la administración empresarial, la seguridad y otras características. Sin embargo, hay importantes diferencias entre las dos versiones. Si bien la edición Enterprise está diseñada para equipos PC, Windows 10 Team está diseñado desde el principio para pantallas de gran tamaño y salas de reuniones. Al evaluar los requisitos de seguridad y administración de Surface Hub, es mejor considerarlo como un nuevo sistema operativo. Este artículo está diseñado para ayudar a destacar las diferencias clave entre Windows 10 Team en Surface Hub y Windows 10 Enterprise y qué significan las diferencias para las organizaciones.

A partir de septiembre de 2020, los clientes tienen la opción de migrar a Windows 10 Pro o Enterprise en Surface Hub 2S. Para conocer más, consulta lo siguiente:

- Anuncio de la disponibilidad de Windows 10 Pro y Enterprise en Surface Hub 2.
- Migrar a Windows 10 Pro o Enterprise en Surface Hub 2

Interfaz de usuario

Shell (interfaz de usuario del sistema operativo)

El shell de Surface Hub está diseñado desde el principio de modo optimizado para pantallas de gran tamaño y táctiles. No usa el mismo shell que Windows 10 Enterprise.

Directivas de la organización que esto puede afectar:

- La configuración relacionada con los controles el shell de Windows 10 Enterprise no se aplica s Surface Hub.

Protector de pantalla y pantalla de bloqueo

Surface Hub no tiene pantalla de bloqueo ni protector de pantalla, pero tiene una característica similar denominada la pantalla de inicio de sesión. La pantalla de inicio muestra las reuniones programadas el calendario de la cuenta del dispositivo y puntos de entrada fácil a las aplicaciones principales de Surface Hub - Skype Empresarial, la Pizarra interactiva y Conectar.

Directivas de la organización que esto puede afectar:

- La configuración de la pantalla de bloqueo, el tiempo de espera de pantalla y el protector de pantalla no se aplican a Surface Hub.

Inicio de sesión de usuario

Surface Hub está diseñado para usarse en espacios comunes, como las salas de reunión. A diferencia de los equipos con Windows, cualquier persona puede acercarse y usar Surface Hub sin iniciar sesión. Para habilitar esta funcionalidad común, Surface Hub no admite el inicio de sesión de Windows, mientras que Windows 10 Enterprise sí lo permite (por ejemplo, iniciar sesión con un usuario en el sistema operativo y usar esas credenciales en todo el sistema operativo). En su lugar, siempre hay un usuario local conectado automáticamente y con privilegios bajos que ha iniciado sesión en Surface Hub. No es compatible con el inicio de sesión de cualquier usuario adicional, incluyendo los usuarios administradores (por ejemplo, cuando un usuario administrador inicia sesión, no han iniciado sesión en el sistema operativo).

Los usuarios pueden iniciar sesión en Surface Hub, pero no iniciarán sesión en el sistema operativo. Por ejemplo, cuando un usuario inicia sesión en Aplicaciones o Mi reuniones y archivos, solo tiene acceso a las

aplicaciones o servicios, no al sistema operativo. Como resultado, el usuario que inició sesión es capaz de recuperar sus archivos y reuniones personales almacenadas de la nube, y estas credenciales se descartan al activar **Finalizar sesión**.

Directivas de la organización que esto puede afectar:

- Por lo general, Surface Hub usa características de bloqueo en lugar del control de acceso de usuario para aplicar la seguridad. Las directivas relacionadas con los requisitos de contraseña, el inicio de sesión interactivo, las cuentas de usuario y el control de acceso no se aplican a Surface Hub.

Guardar y explorar archivos

Los usuarios tienen acceso a un conjunto limitado de directorios en Surface Hub:

- Música
- Vídeos
- Documentos
- Imágenes
- Descargas

Los archivos que se guardan localmente en estos directorios se eliminan cuando los usuarios presionen **Terminar la sesión**. Para guardar contenido creado durante una reunión, los usuarios deben guardar los archivos en una unidad USB o en OneDrive.

Directivas de la organización que esto puede afectar: - Las directivas relacionadas con los permisos de acceso y la propiedad de archivos y carpetas no se aplican a Surface Hub. Los usuarios no pueden explorar ni guardar archivos en directorios del sistema ni carpetas de red.

Aplicaciones

Aplicaciones predeterminadas

Con pocas excepciones, las aplicaciones predeterminadas para la Plataforma universal de Windows (UWP) de Surface Hub también están disponibles en los equipos con Windows 10.

Aplicaciones para UWP instaladas previamente en Surface Hub:

- Alarmas y reloj
- Calculadora
- Conectar
- Excel Mobile
- Centro de opiniones
- Explorador de archivos
- Introducción
- Mapas
- Microsoft Edge
- Microsoft Power BI
- Microsoft Teams
- Microsoft Whiteboard
- OneDrive
- Fotos
- PowerPoint Mobile
- Configuración
- Tienda

- Sugerencias
- Word Mobile

Directivas de la organización que esto puede afectar:

- Usa las directrices de Windows 10 Enterprise para determinar las características y los requisitos de red de las aplicaciones predeterminadas en Surface Hub.

Instalar aplicaciones, controladores y servicios

Para ayudar a mantener la naturaleza del dispositivo, Surface Hub solo admite la instalación de aplicaciones para la Plataforma universal de Windows (UWP) y no admite la instalación de aplicaciones, servicios ni controladores clásicos de Win32. Asimismo, solo los administradores tienen acceso para instalar aplicaciones para UWP.

Directivas de la organización que esto puede afectar:

- Los empleados solo pueden usar las aplicaciones que hayan instalado los administradores, lo que ayuda a mitigar contra un uso no intencionado. Surface Hub no admite la instalación de los agentes de Win32 que la mayoría de las herramientas de administración y supervisión de PC tradicionales.

Seguridad y bloqueo

Para que Surface Hub se use en espacios comunes, como reuniones de las salas, su sistema operativo personalizado implementa muchas de las características de seguridad y bloqueo disponibles en Windows 10. Para obtener más información, vea Surface Hub de seguridad

Surface Hub implementa las siguientes características de seguridad de Windows 10:

- Arranque seguro
- Control de aplicaciones de Windows Defender y protección basada en la virtualización de la integridad del código
- Directivas de restricción de aplicaciones con AppLocker
- Cifrado de unidad BitLocker
- Módulo de plataforma segura (TPM)
- Antivirus de Microsoft Defender en Windows
- Control de cuentas de usuario (UAC) para acceder a la aplicación Configuración

Las siguientes características de Surface Hub proporcionan seguridad adicional:

- Firmware UEFI personalizado
- El shell y el menú Inicio personalizados limitan al dispositivo a las funciones de reunión
- El Explorador de archivos personalizado solo concede acceso a los archivos y las carpetas de Mis documentos
- La aplicación Configuración personalizada solo permite a los administradores modificar la configuración del dispositivo
- La descarga de controladores Plug and Play avanzados está deshabilitada

Directivas de la organización que esto puede afectar:

- Ten en cuenta las siguientes características al realizar la evaluación de seguridad de Surface Hub.

Administración

Configuración de dispositivo

Las opciones del dispositivo se pueden configurar a través de la aplicación Configuración. La aplicación

Configuración está personalizada para Surface Hub, pero también contiene muchas de las opciones de configuración familiares de Windows 10 Escritorio. Un mensaje de Control de cuentas de usuario (UAC) aparece en la pantalla cuando se abre la aplicación Configuración para comprobar las credenciales del administrador, pero este proceso no inicia la sesión del administrador.

Directivas de la organización que esto puede afectar:

- Los empleados pueden usar Surface Hub para reuniones, pero no pueden modificar las opciones de configuración del dispositivo. Además de las características de bloqueo, esto garantiza que los empleados solo usarán el dispositivo para las funciones de reunión.

Características de administración

Las características administrativas de Windows 10 Enterprise, como Microsoft Management Console, Ejecutar, Símbolo del sistema, PowerShell, Editor del registro, Visor de eventos y Administrador de tareas administrativas, no se admiten en Surface Hub. La aplicación Configuración contiene todas las características administrativas disponibles localmente en Surface Hub.

Administración y supervisión remotas

Surface Hub admite la administración remota a través de soluciones de administración de dispositivos móviles (MDM), como Microsoft Intune y supervisión a través de Azure Monitor.

Directivas de la organización que esto puede afectar:

- Surface Hub no admite la instalación de los agentes de Win32 que requiere la mayoría de las herramientas de administración y supervisión de equipos tradicionales, como System Center Operations Manager.

Directiva de grupo

Surface Hub no admite Windows de grupo, incluida la auditoría. En su lugar, usa MDM para aplicar directivas a Surface Hub. Para obtener más información sobre MDM, consulta Administrar la configuración con un proveedor de MDM (Surface Hub).

Directivas de la organización que esto puede afectar:

- Usa MDM para administrar Surface Hub en lugar de directivas de grupo.

Asistencia remota

Surface Hub no admite la asistencia remota.

Directivas de la organización que esto puede afectar:

- Las directivas relacionadas con la asistencia remota no se aplican a Surface Hub.

Red

Unirse a un dominio y unirse Azure Active Directory (Azure AD)

Surface Hub usa la unión a un dominio y la unión a Azure AD principalmente para proporcionar un grupo de administradores respaldados por el directorio. No se admite la combinación híbrida. Los usuarios no pueden iniciar sesión con una cuenta de dominio. Para obtener más información, consulta Administración del grupo de administradores.

Directivas de la organización que esto puede afectar:

- La configuración de directiva de grupo no se aplica cuando Surface Hub se une al dominio. La configuración de directiva relacionada con la pertenencia a un dominio no se aplica a Surface Hub.

Acceder a los recursos de dominio

Los usuarios pueden iniciar sesión en Microsoft Edge para acceder a sitios de intranet y recursos en línea (como Office 365). Si Surface Hub está configurado con una cuenta de dispositivo, el sistema la usa para acceder a

Exchange y Skype Empresarial. Sin embargo, Surface Hub no admite el acceso a recursos de dominio, como recursos compartidos de archivos e impresoras.

Directivas de la organización que esto puede afectar:

- Las directivas relacionadas con el acceso a objetos de dominio no se aplican a Surface Hub.

Datos de diagnóstico

El sistema de operativo de Surface Hub usa el componente Experiencia del usuario y telemetría asociadas de Windows 10 para recopilar y transmitir datos de diagnóstico. Para obtener más información, consulta Configurar los datos de diagnóstico de Windows en la organización.

Directivas de la organización que esto puede afectar:

- Configura los niveles de datos de diagnóstico de Surface Hub de la misma manera que lo harías para Windows 10 Enterprise.

Información técnica para Surface Hub de 55" (v1)

12/01/2022 • 5 minutes to read

Precios	A partir de 8.999 $
Tamaño	31,75" x 59,62" x 3,38" (806,4 mm x 1514,3 mm x 85,8 mm)
Almacenamiento/RAM	SSD de 128 GB con 8 GB de RAM
Procesador	Intel de 4ª generación® Core™ i5
Gráficos	Intel® HD 4600
Puertos	**Equipo interno** • (1) USB 3.0 (inferior) + (1) USB 3.0 (acceso lateral) • (2) USB 2.0 • Ethernet 1000 Base-T • DisplayPort • Salida de vídeo • Salida estéreo de 3,5 mm • Conector RJ11 para el control de nivel del sistema **Equipo alternativo** • (2) Salida USB 2.0 de tipo B • Conexión para cámara, sensores, micrófono, altavoces • (1) Entrada de vídeo DisplayPort **Equipo invitado** • Entrada de vídeo DisplayPort • Entrada de vídeo HDMI • Entrada de vídeo VGA • Entrada estéreo de 3,5 mm • (1) USB 2.0 tipo B Touchback™ salida
Sensores	(2) Sensores pasivos de presencia de infrarrojos, sensores de luz ambiental
Altavoces	(2) Altavoces estéreo frontales
Micrófono	Matriz de 4 elementos de alto rendimiento
Cámara	(2) Cámaras HD en ángulo ancho de 1080p a 30 fps
Lápiz	(2) Precisión de subpíxel con tecnología, activa
Botones del lado físico	Energía, Selección de entrada, Volumen, Brillo
Software	Windows 10 + Office (Word, PowerPoint, Excel)

Qué hay en el cuadro	• Surface Hub 55" • (2) Lápices de Surface Hub • Cable de alimentación • Guía de configuración • Guía de inicio • Documentos de seguridad y garantía • Teclado todo en uno inalámbrico
Características de montaje	4 X VESA estándar, 400 x 400 mm más patrón de 1150 x 400 mm, 8X M6 X 1,0 ubicaciones de montaje en subproceso
Altura de la pantalla desde el plano inferior	Alto recomendado de 55 pulgadas (139,7 cm) al centro de la pantalla
Peso del producto	Aprox. 105 lb (47,6 kilos) sin accesorios
Peso del envío del producto	Aprox. 150 lb (68 kilos)
Dimensiones del producto HxWxD	31,63 x 59,62 x 3,2 pulgadas (80,34 x 151,44 x 8,14 cm)
Dimensiones de envío de productos HxWxD	43 x 65 x 20 pulgadas (109 x 165 x 51 cm)
Grosor del producto	Superficie táctil a superficie de montaje: ≤ 2,4 pulgadas (6 cm)
Orientación	Solo horizontal. La pantalla no se puede usar en orientación vertical.
BTU	1706 BTU/h
Resolución de imagen	1920 x 1080
Velocidad de fotogramas	120Hz
Intervalo preferido de EDID, equipo de reemplazo	Actualización vertical de 1920 x 1080, 120Hz
Sincronización preferida de EDID, conexión por cable	Actualización vertical de 1920 x 1080, 60Hz
Resalte de entrada	(50/60Hz) Nominal de 110/230v, 90-265v máximo
Alimentación de entrada, funcionamiento	Máximo de 500 W
Energía de entrada, modo de espera	Nominal de 5 W

NOTE

Surface Hub se puede usar continuamente durante un máximo de 18 horas al día. Para optimizar la eficiencia, Surface Hub usa sensores inteligentes para desactivar la pantalla LED cuando ya no se detecta la presencia, lo que significa que no es necesario apagarla al final del día. Si la unidad se instala en un entorno de trabajo de 24 horas, los sensores se pueden deshabilitar para cumplir con la recomendación de uso máximo de 18 horas al día. Ten en cuenta que la visualización prolongada de una señal de vídeo puede provocar la grabación o la retención de imágenes en la pantalla. Para obtener más información acerca de la administración de la configuración de energía, vea:

- Administración local para la configuración de Surface Hub
- SurfaceHub CSP: Administración de clientes de Windows

Conexiones de equipo de reemplazo

CONECTOR Y UBICACIÓN	ETIQUETA	DESCRIPCIÓN
Modificador, E/S inferior		Cambia la función entre el uso de un equipo interno o un equipo externo.
Puerto de presentación, E/S inferior		Proporciona entrada para el equipo de reemplazo.
Usb tipo B, E/S inferior		Proporciona conexión USB para el equipo de reemplazo a periféricos internos.
Usb tipo B, E/S inferior		Proporciona conexión USB para el concentrador integrado.

Conexiones de conexión con cable

CONECTOR Y UBICACIÓN	ETIQUETA	DESCRIPCIÓN
Puerto de presentación, E/S inferior		Proporciona entrada para el equipo conectado por cable.
HDMI, E/S inferior		Proporciona una entrada HDMI para el equipo conectado por cable.
VGA, E/S inferior		Proporciona una entrada VGA para conectar el equipo con cable.
3,5 mm, E/S inferior		Proporciona entrada de audio analógico.
Usb tipo B, E/S inferior		Proporciona conexión USB para la entrada táctil de ingesta de vídeo.

Conexiones adicionales

CONECTOR Y UBICACIÓN	ETIQUETA	DESCRIPCIÓN

CONECTOR Y UBICACIÓN	ETIQUETA	DESCRIPCIÓN
Usb de tipo A, E/S lateral		Proporciona 1 conexión USB 3.0 para dispositivos USB. Compatible con USB de activación.
Usb de tipo A, E/S inferior con aislador azul		Proporciona conexión USB 3.0.
3,5 mm, E/S inferior		Proporciona salida de audio analógico.
Puerto de presentación, E/S inferior		Proporciona la función de salida de vídeo reflejada a otra pantalla.
Receptáculo IEC/EN60320-C13 con conmutador duro		Proporciona entrada de AC y cumplimiento con los requisitos de energía de la UE.
RJ45, E/S inferior		Se conecta a Ethernet.
RJ11, E/S inferior		Se conecta a los sistemas de control de la sala.

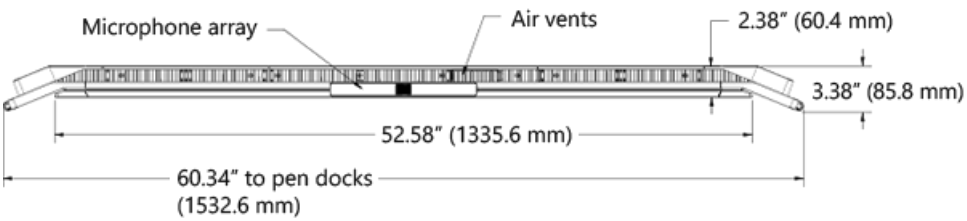
NOTE

Surface Hub se puede usar continuamente durante un máximo de 18 horas al día. Para optimizar la eficiencia, Surface Hub usa sensores inteligentes para desactivar la pantalla LED cuando ya no se detecta la presencia, lo que significa que no es necesario apagarla al final del día. Si la unidad se instala en un entorno de trabajo de 24 horas, los sensores se pueden deshabilitar para cumplir con la recomendación de uso máximo de 18 horas al día. Ten en cuenta que la visualización prolongada de una señal de vídeo puede provocar la grabación o la retención de imágenes en la pantalla. Para obtener más información acerca de la administración de la configuración de energía, vea:

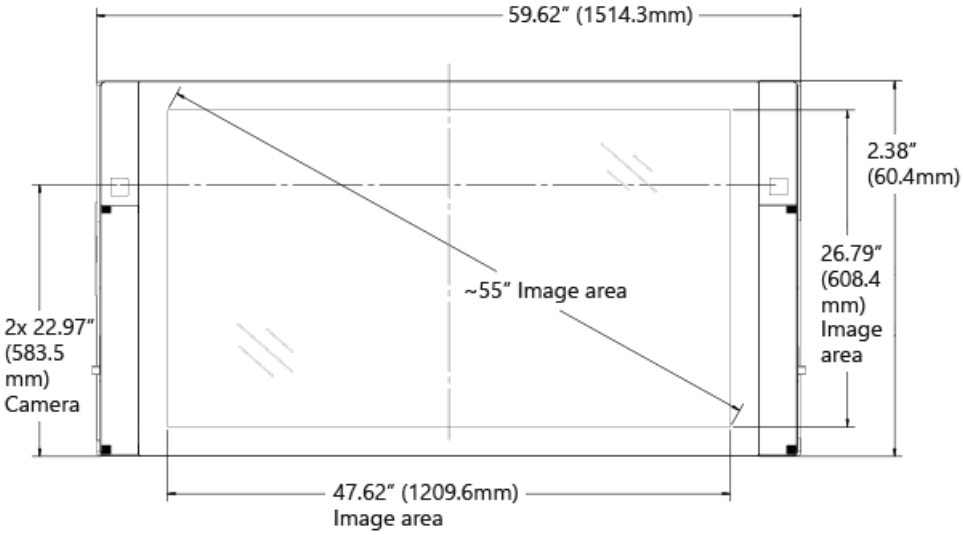
- Administración local para la configuración de Surface Hub
- SurfaceHub CSP: Administración de clientes de Windows

Diagramas de puertos y autorizaciones

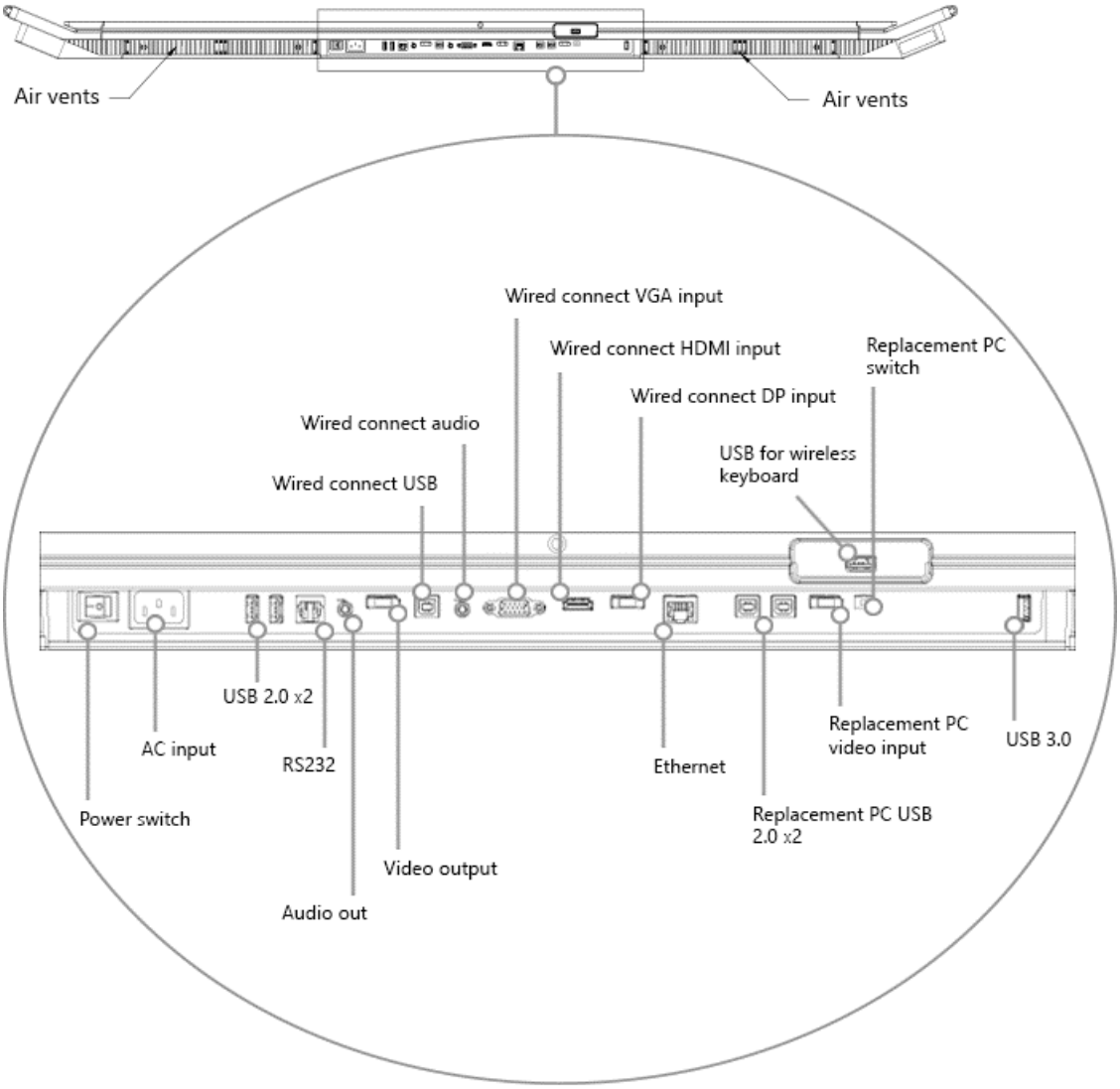
Vista superior de Surface Hub de 55"



Vista frontal de Surface Hub de 55"

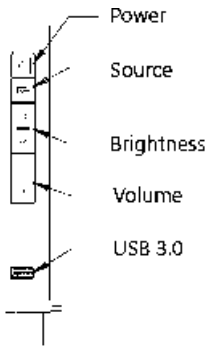


Vista inferior de Surface Hub de 55"

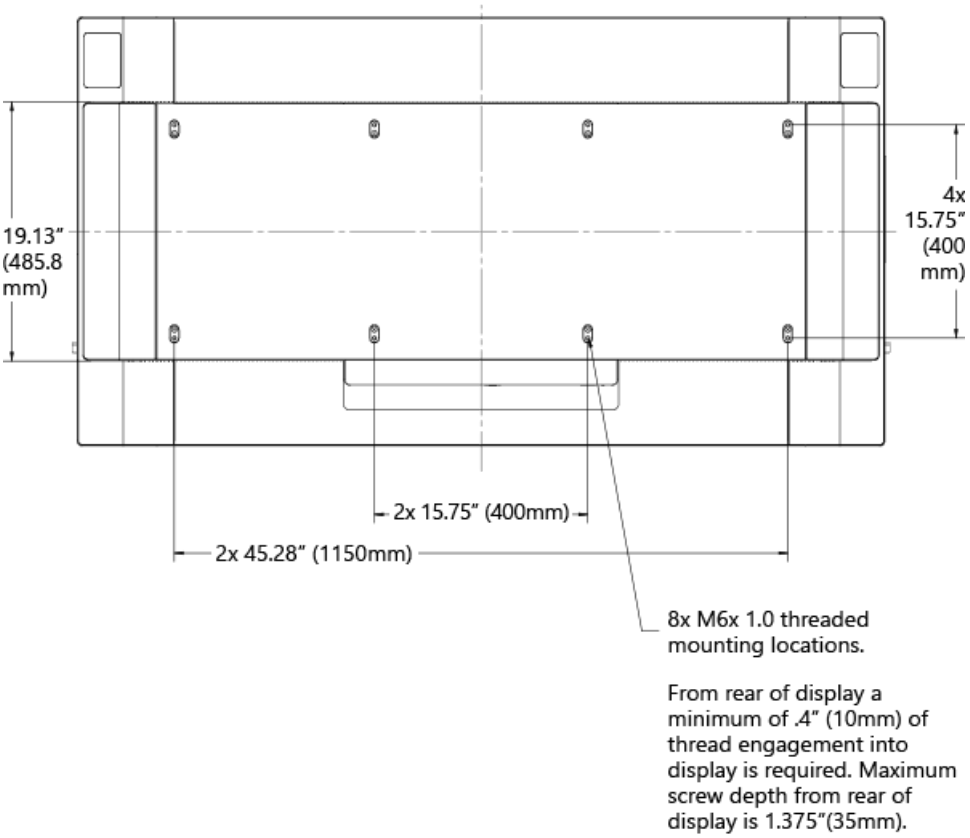


Puertos del equipo de reemplazo en Surface Hub 55".

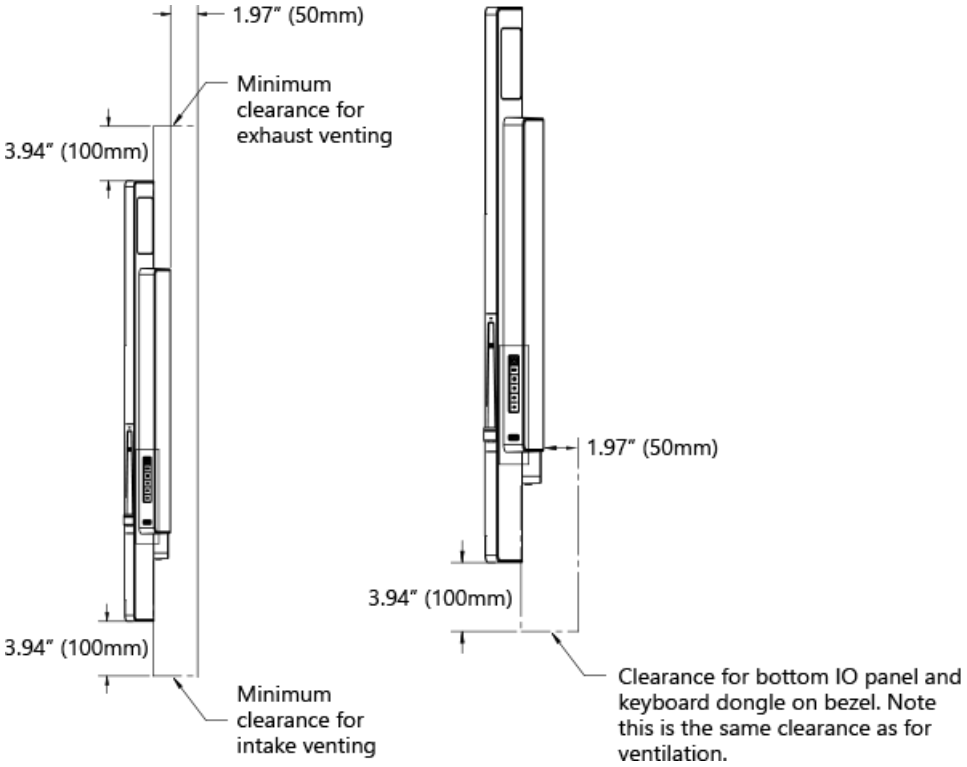
Teclado en el lado derecho de Surface Hub de 55"



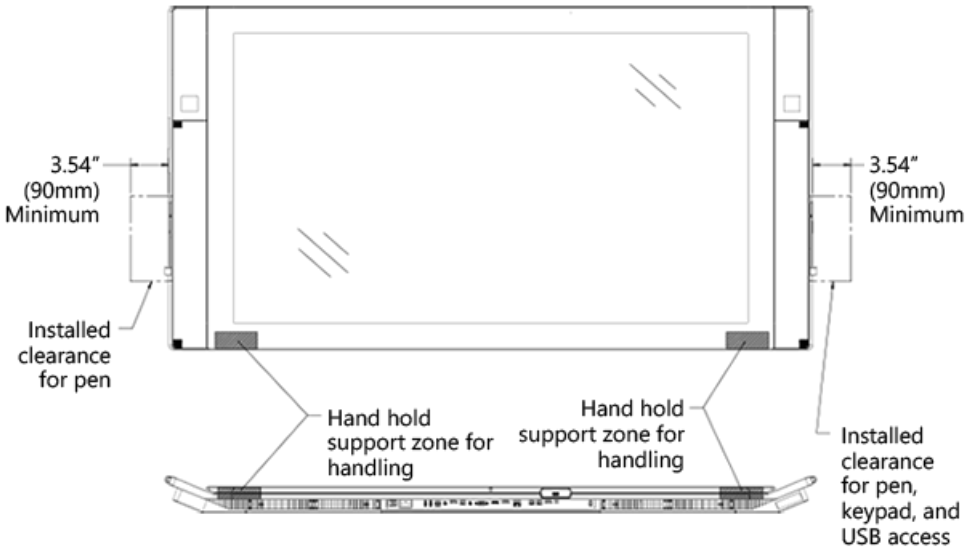
Vista trasera de Surface Hub de 55"



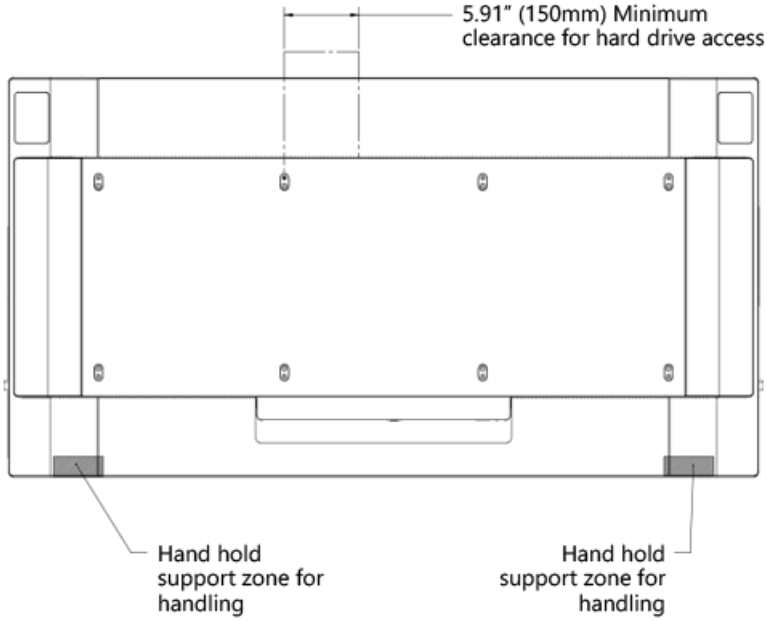
Autorizaciones para Surface Hub de 55"



Retenciones y permisos frontales e inferiores para Surface Hub de 55"



Retenciones y autorizaciones traseras para Surface Hub de 55"


5.91” (150mm) Minimum
clearance for hard drive access
Hand hold
support zone for
handling
Hand hold
support zone for
handling

Información técnica para Surface Hub de 84" (v1)

12/01/2022 • 4 minutes to read

Precios	A partir de 21.999 $
Tamaño	46,12" x 86,7" x 4,15" (1171,5 mm x 2202,9 mm x 105,4 mm)
Almacenamiento/RAM	SSD de 128 GB con 8 GB de RAM
Procesador	Intel de 4ª generación® Core™ i7
Gráficos	NVIDIA Quadro K2200
Puertos	**Equipo interno** • (1) USB 3.0 (inferior) + (1) USB 3.0 (acceso lateral) • (4) USB 2.0 • Ethernet 1000 Base-T • Salida de vídeo DisplayPort • Salida estéreo de 3,5 mm • Conector RJ11 para el control de nivel del sistema **Equipo alternativo** • (2) Salida USB 2.0 tipo B • conexión para cámara, sensores, micrófono, altavoces • (2) Entrada de vídeo DisplayPort **Equipo invitado** • Entrada de vídeo DisplayPort • Entrada de vídeo HDMI • Entrada de vídeo VGA • Entrada estéreo de 3,5 mm • (1) USB 2.0 tipo B Touchback™ salida
Sensores	(2) Sensores pasivos de presencia de infrarrojos, sensores de luz ambiental
Altavoces	(2) Altavoces estéreo frontales
Micrófono	Matriz de 4 elementos de alto rendimiento
Cámara	(2) Cámaras HD en ángulo ancho de 1080p a 30 fps
Lápiz	(2) Precisión de subpíxel con tecnología, activa
Botones del lado físico	Energía, Selección de entrada, Volumen, Brillo
Software	Windows 10 + Office (Word, PowerPoint, Excel)

Qué hay en el cuadro	• Surface Hub 84" • (2) Lápices de Surface Hub • Cable de alimentación • Guía de configuración • Documentos de seguridad y garantía • Teclado todo en uno inalámbrico
Características de montaje	4X VESA estándar, patrón de 1200 x 600 mm, 8X M8 X 1,25 ubicaciones de montaje en subproceso
Altura de la pantalla desde el plano inferior	Alto recomendado de 54 pulgadas (139,7 cm) al centro de la pantalla
Peso del producto	Aprox. 280 lb (127 kilos).
Peso del envío del producto	Aprox. 580 lb (263 kilos).
Dimensiones del producto HxWxD	46 x 86,9 x 4,1 pulgadas (116,8 x 220,6 x 10,4 cm)
Dimensiones de envío de productos HxWxD	66,14 x 88,19 x 24,4 pulgadas (168 x 224 x 62 cm)
Grosor del producto	Superficie táctil a superficie de montaje: ≤ 3,1 pulgadas (7,8 cm)
Orientación	Solo horizontal. La pantalla no se puede usar en orientación vertical.
BTU	3070,8 BTU/h
Resolución de imagen	3840 x 2160
Velocidad de fotogramas	120Hz
Relación de contraste	1400:1
Intervalo preferido de EDID, equipo de reemplazo	Actualización vertical de 3840 x 2140 y 120Hz
Sincronización preferida de EDID, conexión por cable	Actualización vertical de 1920 x 1080, 60Hz
Resalte de entrada	Nominal de 110/230v, 90-265v max
Alimentación de entrada, funcionamiento	Máximo de 900 W
Energía de entrada, espera	5W nominal, 1-10W max

NOTE

Surface Hub se puede usar continuamente durante un máximo de 18 horas al día. Para optimizar la eficiencia, Surface Hub usa sensores inteligentes para desactivar la pantalla LED cuando ya no se detecta la presencia, lo que significa que no es necesario apagarla al final del día. Si la unidad se instala en un entorno de trabajo de 24 horas, los sensores se pueden deshabilitar para cumplir con la recomendación de uso máximo de 18 horas al día. Ten en cuenta que la visualización prolongada de una señal de vídeo puede provocar la grabación o la retención de imágenes en la pantalla. Para obtener más información sobre cómo administrar la configuración de energía, vea:

- Administración local para la configuración de Surface Hub
- SurfaceHub CSP: Administración de clientes de Windows

Conexiones de equipo de reemplazo

CONECTOR Y UBICACIÓN	ETIQUETA	DESCRIPCIÓN
Modificador, E/S inferior		Cambia la función entre el uso de un equipo interno o un equipo externo.
Puerto de presentación, E/S inferior		Proporciona entrada para el equipo de reemplazo.
Puerto de presentación, E/S inferior		Proporciona la segunda entrada para el equipo de reemplazo.
Usb tipo B, E/S inferior		Proporciona conexión USB para el equipo de reemplazo a periféricos internos.
Usb tipo B, E/S inferior		Proporciona conexión USB para el concentrador integrado.

Conexiones de conexión con cable

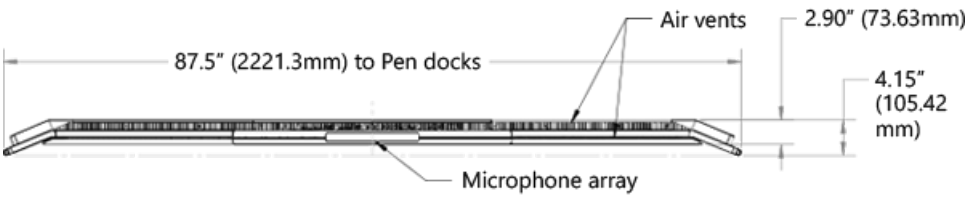
CONECTOR Y UBICACIÓN	ETIQUETA	DESCRIPCIÓN
Puerto de presentación, E/S inferior		Proporciona entrada para el equipo conectado por cable.
HDMI, E/S inferior		Proporciona una entrada HDMI para el equipo conectado por cable.
VGA, E/S inferior		Proporciona entrada VGA para el equipo conectado con cable.
3,5 mm, E/S inferior		Proporciona entrada de audio analógico.
Usb tipo B, E/S inferior		Proporciona conexión USB para la entrada táctil de ingesta de vídeo.

Conexiones adicionales

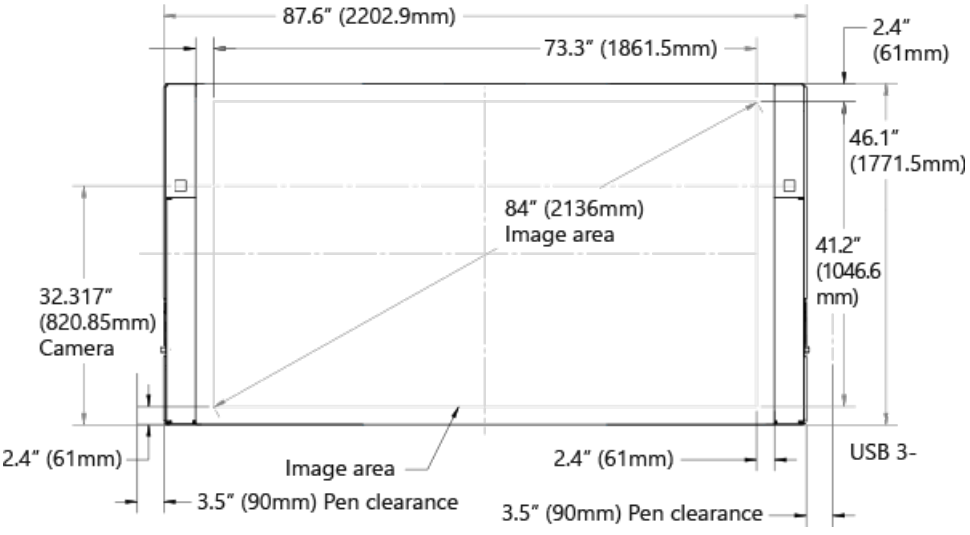
CONECTOR Y UBICACIÓN	ETIQUETA	DESCRIPCIÓN
Tipo USB A, E/S lateral		Proporciona 1 conexión USB 3.0 para dispositivos USB. Compatible con USB de activación.
Usb de tipo A, E/S inferior con aislador azul		Proporciona conexión USB 3.0.
3,5 mm, E/S inferior		Proporciona salida de audio analógico.
Puerto de presentación, E/S inferior		Proporciona la función de salida de vídeo reflejada a otra pantalla.
Receptáculo IEC/EN60320-C13 con conmutador duro		Proporciona entrada de AC y cumplimiento con los requisitos de energía de la UE.
RJ45, E/S inferior		Se conecta a Ethernet.
RJ11, E/S inferior		Se conecta a los sistemas de control de la sala.

Diagramas de puertos y autorizaciones

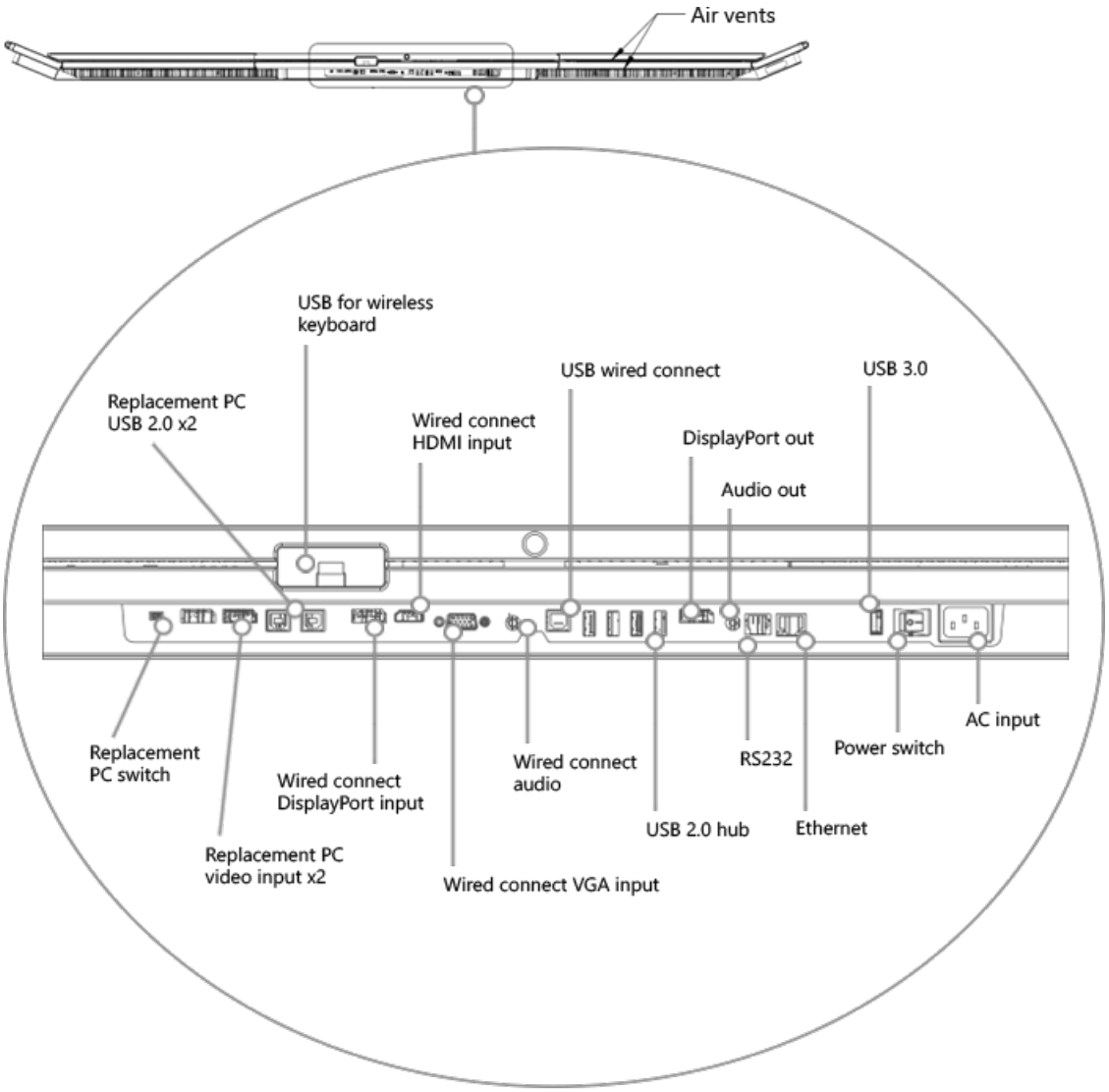
Vista superior de Surface Hub de 84"



Vista frontal de Surface Hub de 84"

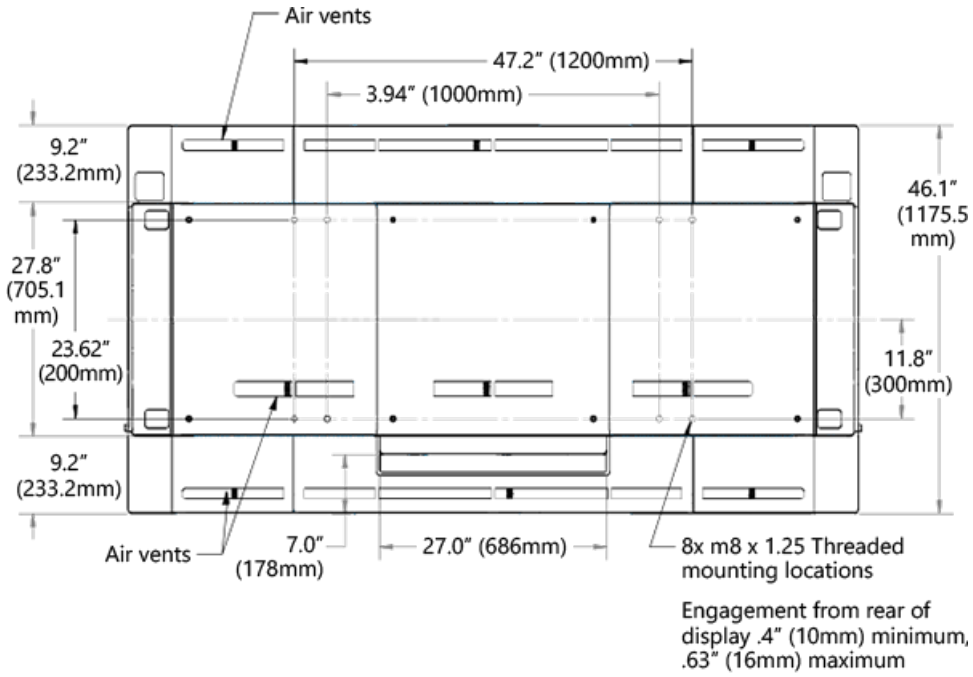


Vista inferior de Surface Hub de 84"

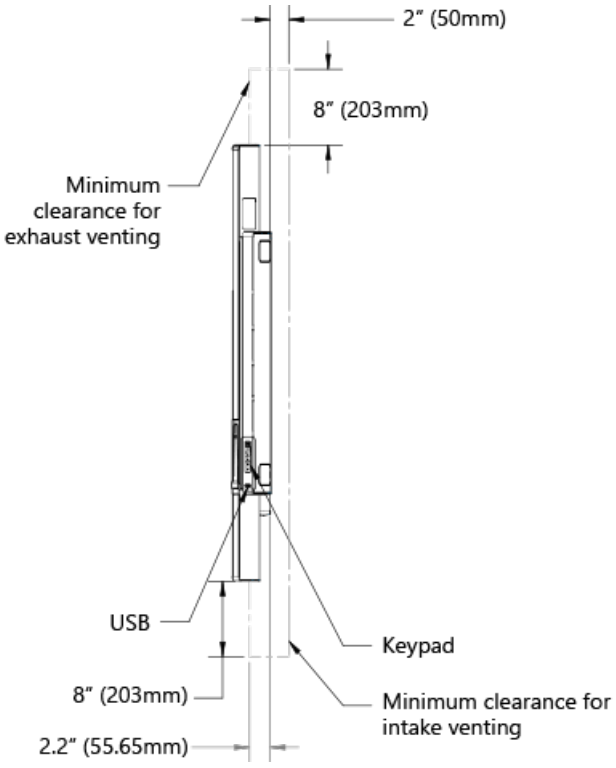


Puertos del equipo de reemplazo en Surface Hub 84".

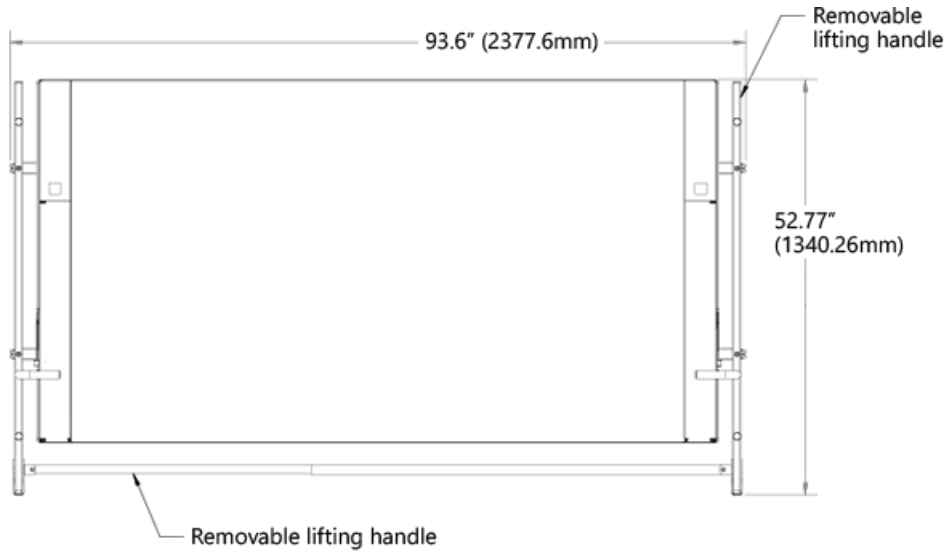
Vista trasera de Surface Hub de 84"



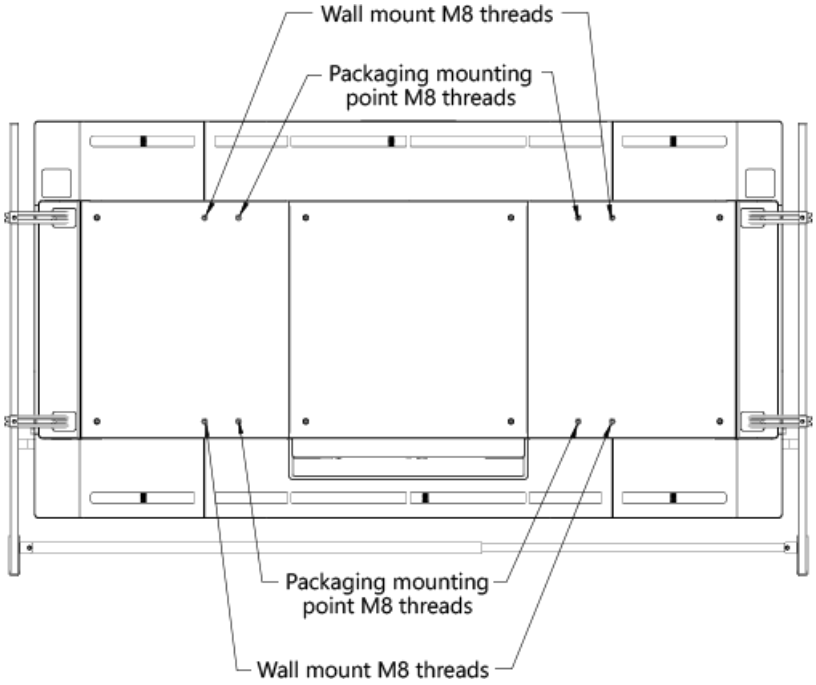
Autorizaciones para Surface Hub de 84"



Controladores de elevación extraíbles en Surface Hub de 84"

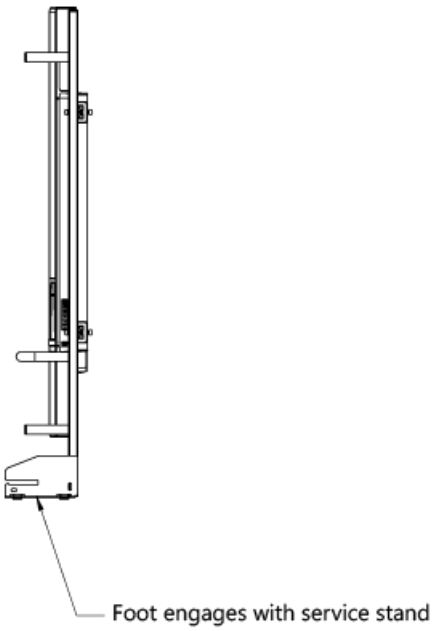


Subprocesos de montaje en pared en la parte posterior de Surface Hub de 84"



Asas de elevación en la vista superior de Surface Hub de 84"

Vista lateral de Surface Hub de 84"


Foot engages with service stand

Normativa general de privacidad de datos y Surface Hub

12/01/2022 • 2 minutes to read

En mayo de 2018, se aprobaba una ley de privacidad europea, el Reglamento general de protección de datos (RGPD). El RGPD impone nuevas reglas a las empresas, las agencias gubernamentales, las organizaciones sin ánimo de lucro y otras organizaciones que ofrecen bienes y servicios a personas de la Unión Europea (UE) o que recopilan y analizan datos vinculados a residentes de la UE.

Surface Hub clientes preocupados por la privacidad en virtud de las nuevas normativas del RGPD pueden administrar la privacidad de sus dispositivos con las siguientes opciones proporcionadas por Microsoft:

- **Opción 1: Surface Hub** dispositivos en regiones que se alocución en las regulaciones del RGPD reducen automáticamente la emisión de datos de diagnóstico a básico. Los clientes que opten por proporcionar un mayor nivel de datos de diagnóstico pueden usar la aplicación Surface Hub Configuración o la administración de dispositivos móviles para invalidar la configuración básica predeterminada.
- **Opción 2: Surface Hub** los clientes que desean quitar los datos de diagnóstico existentes pueden descargar la Surface Hub **eliminar** datos de diagnóstico desde el Microsoft Store. Esta aplicación permitirá a los clientes solicitar la eliminación de datos de diagnóstico asociados directamente desde Surface Hub dispositivo.

Microsoft tiene una amplia experiencia en la protección de datos, la protección de la privacidad y el cumplimiento de normativas complejas, y actualmente cumple con las cláusulas del Escudo de privacidad ue-EE. UU. y modelo de la UE. Creemos que el RGPD es un paso adelante importante para aclarar y habilitar los derechos de privacidad individuales. Queremos ayudarle a centrarse en su negocio principal a la vez que se prepara de forma eficaz para el RGPD.

Preparar el entorno para Microsoft Surface Hub

12/01/2022 • 5 minutes to read

En esta página se describen las dependencias para configurar y administrar Surface Hub v1 o Surface Hub 2S.

Dependencias de infraestructura

Revisa estas dependencias para asegurarte de que las características de Surface Hub funcionarán en tu infraestructura de TI.

DEPENDENCIA	DESCRIPCIÓN	OBTÉN MÁS INFORMACIÓN
Servicios locales y Active Directory o M365	Surface Hub usa una cuenta de Active Directory o Azure AD (denominada cuenta de **dispositivo)** para obtener acceso a Exchange y Teams (o Skype Empresarial). Surface Hub debe ser capaz de conectarse al controlador de dominio de Active Directory o al inquilino de Azure AD para validar las credenciales de la cuenta del dispositivo, así como para acceder a información como el nombre para mostrar de la cuenta del dispositivo, el alias, el servidor Exchange y la dirección de Protocolo de inicio de sesión (SIP). **NOTA: Surface Hubs funciona con Microsoft Teams, Skype Empresarial Server 2019, Skype Empresarial Server 2015 o Skype Empresarial Online. No se admiten plataformas anteriores, como Lync Server 2013. Los Surface Hubs no se admiten GCC entornos De alto o DoD.**	Microsoft 365 de conexión Crear y probar una cuenta de dispositivo
Windows Actualización, almacenamiento y diagnóstico	El acceso a Windows Update o Windows Update para empresas es necesario para mantener Surface Hub actualizaciones de calidad y características del sistema operativo. El acceso a la Microsoft Store es necesario para mantener las aplicaciones.	Administrar puntos de conexión de conexión para Windows 10 Enterprise, versión 20H2 Administrar actualizaciones de Windows en Surface Hub
Solución de administración de dispositivos móviles (MDM) (Microsoft Intune, Microsoft Endpoint Configuration Manager o proveedor MDM compatible con terceros)	Si quieres aplicar la configuración e instalar las aplicaciones de forma remota, y hacerlo en varios dispositivos a la vez, debes configurar una solución MDM e inscribir el dispositivo en dicha solución.	Puntos de conexión de la red para Microsoft Intune Administrar la configuración con un proveedor de MDM

DEPENDENCIA	DESCRIPCIÓN	OBTÉN MÁS INFORMACIÓN
Azure Monitor	Azure Monitor se puede usar para supervisar el estado de Surface Hub dispositivos. **NOTA: Los Surface Hubs no admiten actualmente el uso de un servidor proxy para comunicarse con el servicio log analytics que usa Azure Monitor.**	Puntos de conexión de Log Analytics Supervisar Surface Hubs con Azure Monitor para realizar un seguimiento de su estado.
Acceso a la red	Los Surface Hub admiten conexiones cableadas o inalámbricas (se prefiere una conexión por cable). **Autenticación 802.1X** En Windows 10 Team 20H2, aunque la autenticación 802.1X para conexiones cableadas e inalámbricas está habilitada de forma predeterminada, debe asegurarse de que un certificado de autenticación y perfil de red 802.1x también esté instalado en Surface Hub. Si administras Surface Hub intune u otra solución de administración de dispositivos móviles, puedes entregar el certificado mediante el CSP ClientCertificateInstall. De lo contrario, puedes crear un paquete de aprovisionamiento e instalarlo durante la instalación de la primera ejecución o mediante la Configuración aplicación. Cuando se aplica el certificado, la autenticación 802.1X comienza automáticamente. **IP dinámica** Surface Hubs no se puede configurar para usar una IP estática. Se les debe asignar una dirección IP a través de DHCP. **Puertos** El Surface Hub requiere los siguientes puertos abiertos: HTTPS: 443 HTTP: 80 NTP: 123	Habilitar la autenticación por cable 802.1x Crear paquetes de aprovisionamiento para Surface Hub

Afiliación de dispositivos

Usa la afiliación a dispositivos para administrar el acceso de los usuarios a Configuración aplicación en Surface Hub. Con el Windows 10 Team operativo (que se ejecuta en Surface Hub), solo los usuarios autorizados pueden ajustar la configuración con la Configuración aplicación. Dado que elegir la afiliación puede afectar a la disponibilidad de las características, planee correctamente para garantizar que los usuarios puedan acceder a las características según lo previsto.

> **NOTE**
> Solo puedes establecer la afiliación de dispositivos durante la configuración inicial de la experiencia de inicio de la caja (OOBE). Si necesitas restablecer la afiliación a dispositivos, tendrás que repetir la configuración de OOBE.

Sin afiliación

Ninguna afiliación es como tener Surface Hub en un grupo de trabajo con una cuenta de administrador local diferente en cada Surface Hub. Si eliges Sin afiliación, debes guardar localmente la clave de BitLocker en una unidad usb. Todavía puedes inscribir el dispositivo con Intune; sin embargo, solo el administrador local puede acceder a la Configuración con las credenciales de cuenta configuradas durante OOBE. Puedes cambiar la contraseña de la cuenta de administrador desde la Configuración aplicación.

Active Directory Domain Services

Si te afilias Surface Hub con los Servicios de dominio de Active Directory locales, debes administrar el acceso a la aplicación Configuración mediante un grupo de seguridad en tu dominio. Esto ayuda a garantizar que todos los miembros del grupo de seguridad tengan permisos para cambiar la configuración en Surface Hub. Tenga en cuenta lo siguiente: cuando Surface Hub filiales con los Servicios de dominio de Active Directory locales, la clave de BitLocker se puede guardar en el esquema de Active Directory. Para obtener más información, vea Prepare your organization for BitLocker: Planning and policies.

Las CA raíz de confianza de la organización se insertan en el mismo contenedor de Surface Hub, lo que significa que no es necesario importarlas mediante un paquete de aprovisionamiento.

Todavía puedes inscribir el dispositivo con Intune para administrar la configuración de forma centralizada en tu Surface Hub.

Azure Active Directory

Cuando eliges asociar tu Surface Hub con Azure Active Directory (Azure AD), cualquier usuario con el rol Administrador global puede iniciar sesión en la aplicación Configuración en Surface Hub. También puedes configurar cuentas de administrador no globales que limiten los permisos a la administración de la aplicación Configuración en Surface Hub. Esto te permite tener en cuenta los permisos de administrador solo para Surface Hubs y evitar el acceso de administrador potencialmente no deseado en todo un dominio de Azure AD.

Si habilitaste la inscripción automática de Intune para tu organización, el Surface Hub se inscribirá automáticamente en Intune; en este escenario, la cuenta usada para la afiliación de Azure AD durante la instalación debe tener licencia para Intune y tener permisos para inscribir Windows dispositivos. Una vez completado el proceso de configuración, la clave BitLocker del dispositivo se guarda automáticamente en Azure AD.

Para obtener más información sobre cómo administrar Surface Hub con Azure AD, consulte:

- Administración del grupo de administradores
- Configurar cuentas de administrador no globales en Surface Hub

Revisar y completar la hoja de cálculo del programa de instalación de Surface Hub (opcional)

Cuando sigas los pasos del programa de primera ejecución de Surface Hub, tendrás que proporcionar determinada información. La hoja de cálculo del programa de instalación resume esa información y proporciona listas de información específica del entorno que necesitarás cuando sigas los pasos del programa de primera ejecución. Para obtener más información, consulta Hoja de cálculo del programa de instalación.

Guía de preparación de sitios para Surface Hub

12/01/2022 • 6 minutes to read

Use esta guía de preparación del sitio para ayudar a planear la instalación de Surface Hub. En esta guía, encontrarás lo siguiente:

- Temas de preparación de sitios
- Especificaciones de hardware detalladas en energía, puertos y cables
- Recomendaciones para mover y almacenar
- Vínculos a instrucciones para desempaquetar y montar

Planeación de la disponibilidad de sitios

El salón debe ser lo suficientemente grande como para proporcionar un buen ángulo de visión, pero lo suficientemente pequeño como para que los micrófonos recojan señales claras de las personas que están en el salón. La mayoría de las habitaciones de aproximadamente 22 metros (siete metros) le proporcionarán una buena experiencia de reunión. En el área de conferencia, Monte Surface Hub donde:

- Todas las personas de la sala pueden verla.
- Los usuarios pueden llegar a los cuatro bordes de la pantalla táctil.
- La pantalla no está en la luz solar directa, lo cual puede afectar a la visualización o dañar la pantalla.
- Las aberturas de ventilación no están bloqueadas.
- Los micrófonos no se ven afectados por las fuentes de ruido, como los ventiladores o los orificios de ventilación. Puede encontrar más detalles en 55 las secciones de información técnica de Microsoft Surface Hub Hub o de 84 " Microsoft Surface Hub. Para obtener información sobre limpieza, cuidado y seguridad, consulte las guías de montaje y la guía para usuarios en https://www.microsoft.com/surface/support/surface-hub .

Consideraciones de hardware

Surface Hub llega con:

- Dos lápices de Surface Hub de Microsoft
- Un teclado inalámbrico de Microsoft, personalizado para Surface Hub
- Un cable de alimentación de 9 metros NEMA 5-15P (estándar de Estados Unidos) a C13

Deberás proporcionar lo siguiente:

- Cables de red CAT-5e o CAT-6
- Cables de pantalla (opcional)
- Cable de audio (opcional)
- Escribe un cable USB a B (opcional)

Para obtener más información acerca de los puertos de cable, consulte 55 las secciones de información técnica de Microsoft Surface Hub Hub o de 84 " Microsoft Surface Hub. Para obtener más información sobre cables, consulte conexión por cable.

Microsoft Surface Hub tiene un equipo interno y no requiere un sistema informático externo.

Para obtener recomendaciones de energía, consulte 55 "información técnica de Microsoft Surface Hub o 84" información técnica de Microsoft Surface Hub. Para las advertencias de seguridad del cable de alimentación, consulte las guías de montaje en https://www.microsoft.com/surface/support/surface-hub .

Datos y otras conexiones

Para usar Surface Hub, necesita un puerto Ethernet activo y una toma de corriente estándar. Además, es posible que desee:

- Equipar la tabla de conferencias para conectarla por cable.
- Expanda la configuración de la toma de pared para incluir:
  - Salidas de CA adicionales
  - Ethernetports
  - Puertos de audio
  - Puertos de vídeo (DisplayPort, HDMI, VGA, etc.)

Cuando llega Surface Hub

Surface Hub es grande y grande, así que puedes avisar cuando llegue y saber qué debe hacer para manejarlo de manera segura. Para obtener más información sobre los pesos de embalaje y otras especificaciones, consulte 55 "información técnica de Microsoft Surface Hub o 84" información técnica de Microsoft Surface Hub.

Considere lo siguiente:

- Espera a desempaquetar Surface hub del contenedor de envíos hasta que lo haya movido al área de conferencia en la que planeas instalarlo.
- Asegúrese de que el muelle de carga acepte un envío en un palet y manténgalo seguro hasta que se pueda instalar.
- Consulte las reglas de la Unión laboral local que requieren que use mano de obra de Unión para descargar o mover Surface Hub.
- No deje Surface Hub en un entorno caliente o húmedo. Al igual que con cualquier equipo informático o de pantalla, el calor y la humedad pueden dañar Surface Hub. Las temperaturas de almacenamiento recomendadas son de 32 a 95 ° f, con una humedad relativa de menos del 70 por ciento.

Surface Hub en movimiento

Antes de mover Surface Hub, asegúrate de que todas las puertas, umbrales, vestíbulos y ascensores sean lo suficientemente grandes como para acomodarlo. Para obtener información sobre las dimensiones y el peso de su Surface Hub en su contenedor de envío, consulte 55 "información técnica de Microsoft Surface Hub o 84" información técnica de Microsoft Surface Hub.

Desembalar Surface Hub

Para desembalar la información, consulta la guía de desembalaje incluida en el contenedor de envío. Puedes abrir las instrucciones de desembalaje antes de abrir el contenedor de envío. Estas instrucciones también pueden encontrarse aquí:https://www.microsoft.com/surface/support/surface-hub

> **IMPORTANT**
> Conserva y almacena todos los materiales de envío de Surface Hub, incluidos el pallet, el contenedor y los tornillos, en caso de que tengas que enviar Surface Hub a una nueva ubicación o enviarlo para su reparación. Para el Surface Hub de 84, conserve los controladores de elevación.

Surface Hub de elevación

El Surface Hub de 55 requiere dos personas para levantar y montar de forma segura. El Surface Hub de 84 requiere cuatro personas para levantar y montar con seguridad. Esos ayudantes deben poder levantar 70 libras a la altura de waist. Para obtener información sobre cómo levantar Surface Hub, consulta la guía de desembalaje y de montaje. Puedes encontrarla en https://www.microsoft.com/surface/support/surface-hub .

Montar y configurar

Para obtener instrucciones detalladas, consulta la guía de montaje https://www.microsoft.com/surface/support/surface-hub .

Hay tres formas de montar Surface Hub:

- **Montaje en pared**: te permite bloquear Surface Hub de forma permanente en una pared de espacio en conferencia.
- **Soporte para el piso montar**: admite Surface Hub en el piso mientras está anclado a un muro de espacios de conferencia.
- **Soporte rodante**: admite Surface Hub y le permite moverlo a otras ubicaciones de conferencia. Para obtener vínculos a guías que proporcionan detalles sobre cada método de montaje, incluidos los requisitos de creación, consulte https://www.microsoft.com/surface/support/surface-hub .

Para obtener especificaciones sobre los montajes disponibles para el Surface Hub original, consulte lo siguiente:

- Hoja de la hoja de remontaje y resalte Surface Hub
- Especificaciones de soporte de Surface Hub y de montaje en pared

La experiencia de conexión

Conectar permite a las personas proyectar el portátil, la tableta o el teléfono en la pantalla de Surface Hub. Conectar permite tipos de conexión inalámbrica o cableada.

Conexión inalámbrica

Como Wireless Connect se basa en Miracast, no necesita cables ni una planificación de configuración adicional para usarlo. Los usuarios pueden cargar Miracast en la mayoría de los dispositivos Windows 8,1 y Windows 10 habilitados para Miracast. Después, pueden proyectar su visualización desde el equipo o el teléfono a la pantalla Surface Hub.

Conexión cableada

Con la conexión por cable, un cable transmite información de equipos, tabletas o teléfonos a Surface Hub. Existen tres opciones de cable de video y todas usan el mismo cable USB 2,0. El paquete de cable puede incluir una o todas estas opciones de conexión.

- DisplayPort (cable de DisplayPort + cable USB 2,0)
- HDMI (cable HDMI + cable USB 2,0)
- VGA (cable VGA + Cable de audio de 3,5 mm + cable USB 2,0)

Por ejemplo, para proporcionar funciones de audio, vídeo y Touchback a las tres opciones de video, el paquete de cable de conexión por cable debe incluir:

- Un cable de DisplayPort
- Un cable HDMI
- Un cable VGA
- Un cable USB 2,0
- Un cable de 3,5 mm

Cuando cree los paquetes de cable de conexión por cable, consulte la 55 "información técnica de Microsoft Surface Hub o 84" secciones de información técnica de Microsoft Surface Hub para obtener detalles técnicos y físicos específicos y ubicaciones de puertos para cada tipo de Surface Hub. Haz que los cables sean lo suficientemente largos para llegar desde Surface Hub hasta donde quiera que el moderador se sienta o se destaque.

Para obtener más información sobre Touchback y Inkback, consulte la guía para usuarios en

https://www.microsoft.com/surface/support/surface-hub .

Consulte también

Ver el vídeo (se abre en un reproductor multimedia emergente)

Instalar Microsoft Surface Hub físicamente

12/01/2022 • 2 minutes to read

La Guía de disponibilidad de Surface Hub de Microsoft le ayudará a asegurarse de que su sitio está listo para la instalación. Incluye información de planificación para los dispositivos de 55" y de 84", así como información sobre cómo mover Surface Hub desde su recepción a la ubicación de instalación, opciones de montaje y una lista de lo que hay en la caja.

También puedes consultar la Guía de desembalaje. Mostrará cómo desempaquetar los dispositivos de forma efectiva y segura. Hay dos guías, una para el de 55" y otra para el de 84". Hay una versión impresa de la Guía de desembalaje adjunta a la parte frontal de la caja de envío de cada unidad.

- Descargar la Guía de desembalaje de 55" desde el Centro de descarga de Microsoft.
- Descargar la versión de 84" desde el Centro de descarga de Microsoft.

Recursos descargables para Surface Hub preparación

12/01/2022 • 2 minutes to read

En este tema se proporcionan vínculos a documentos Surface Hub útiles, como hojas de datos del producto y la guía del usuario.

VÍNCULO	DESCRIPCIÓN
Guía de instalación de Surface Hub (español, francés, inglés) (PDF)	Obtén una breve introducción acerca de cómo configurar el entorno para tu nuevo Surface Hub.
Manual de referencia rápida de Surface Hub (PDF)	Usa este manual de referencia rápida para obtener información acerca de las características y funciones clave de Surface Hub.
Manual del usuario de Surface Hub (PDF)	Aprende a usar Surface Hub para reuniones programadas y ad hoc. Invita a participantes remotos, usa las herramientas integradas, guarda los datos de tu reunión y mucho más.
Controladores de equipo sustituto para Surface Hub	El conjunto de controladores de equipo sustituto para Surface Hub está disponible para los clientes que han optado por deshabilitar el PC interno de Surface Hub y usar un PC externo con su Surface Hub de 84" o 55". Esta descarga está diseñada para usarse con el Manual de administración de Surface Hub, en el que se incluyen detalles adicionales acerca de la configuración de un equipo sustituto para Surface Hub.
Kit de implementación y uso correctos de Microsoft Surface Hub (ZIP)	Prácticas recomendadas para generar conocimientos e implementar la administración de cambios con el objetivo de maximizar la adopción, el uso y las ventajas de Microsoft Surface Hub. En el archivo ZIP Kit de implementación y uso correctos se incluye el documento detallado Kit de implementación y uso correctos, una presentación acerca de Surface Hub, asistencia para demostraciones, gráficos de conocimientos y mucho más.
Manual de desembalaje para Surface Hub de 84" (PDF)	Aprende a desembalar tu Surface Hub de 84" de manera eficaz y segura. Ver el vídeo (se abre en un reproductor multimedia emergente)
Manual de desembalaje para Surface Hub de 55" (PDF)	Aprende a desembalar tu Surface Hub de 55" de manera eficaz y segura. Ver el vídeo (se abre en un reproductor multimedia emergente)
Manual de montaje en la pared y ensamblado (PDF)	Obtén instrucciones detalladas acerca de cómo ensamblar las abrazaderas de pared y montar el Surface Hub en ellas de manera segura y firme. Ver el vídeo (se abre en un reproductor multimedia emergente)

VÍNCULO	DESCRIPCIÓN
Manual de montaje en el suelo y ensamblado (PDF)	Obtén instrucciones detalladas sobre cómo ensamblar las abrazaderas de suelo y montar Surface Hub en ellas de manera segura y firme. Ver el vídeo (se abre en un reproductor multimedia emergente)
Manual de montaje en soporte móvil y ensamblado (PDF)	Obtén instrucciones detalladas acerca de cómo ensamblar el soporte móvil y montar el Surface Hub en él de manera segura y firme. Ver el vídeo (se abre en un reproductor multimedia emergente)
Hoja de datos de los montajes y soportes (PDF)	Especificaciones y precios de todos los montajes y soportes complementarios del Surface Hub que convierten el área de trabajo en un área de trabajo de Surface Hub.
Especificaciones de los montajes en pared y los soportes de Surface Hub (PDF)	Especificaciones ilustradas de los soportes móviles, montajes de pared y montajes de suelo para el Surface Hub de 55" y 84".

Administración de grupos de administración para Surface Hub

12/01/2022 • 4 minutes to read

Cada Surface Hub se puede configurar localmente mediante la aplicación Configuración en el dispositivo. Para impedir que usuarios no autorizados cambien la configuración, la aplicación Configuración requiere credenciales de administrador para abrir la aplicación.

Administración del grupo de administradores

Puedes configurar cuentas de administrador para el dispositivo de las siguientes maneras:

- Crear una cuenta de administrador local
- Unir el dispositivo a Active Directory
- Azure AD unirse al dispositivo
- Configurar cuentas de administrador no globales en Azure AD unidos (Surface Hub 2S)

Crear una cuenta de administrador local

Para crear un administrador local, elige usar un administrador local durante la primera ejecución. De este modo, se creará una cuenta de administrador local única en Surface Hub con el nombre de usuario y la contraseña de tu elección. Usa estas credenciales para abrir la aplicación Configuración.

Ten en cuenta que la información de cuenta de administrador local no está respaldada por ningún servicio de directorio. Te recomendamos que elijas solo un administrador local si el dispositivo no tiene acceso a Active Directory (AD) o Azure Active Directory (Azure AD). Si decides cambiar la contraseña del administrador local, puedes hacerlo en Configuración. Sin embargo, si quieres cambiar de una cuenta de administrador local a un grupo de tu dominio o inquilino de Azure AD, tendrás que restablecer el dispositivo y volver a ejecutar el programa como la primera vez.

Unir el dispositivo a Active Directory

Puedes unir Surface Hub a tu dominio de AD para permitir que los usuarios de un grupo de seguridad especificado puedan configurar los parámetros. Durante la primera ejecución, elige usar los servicios de dominio de Active Directory. Deberás proporcionar las credenciales que son capaces de unir el dominio de tu elección y el nombre de un grupo de seguridad existente. Cualquier persona que sea miembro de ese grupo de seguridad puede escribir sus credenciales y desbloquear Configuración.

¿Qué sucede cuando unes tu Surface Hub a un dominio?

Los Surface Hubs usan unión a un dominio para:

- Conceder derechos de administrador a los miembros de un grupo de seguridad especificado en AD.
- Copia de seguridad de la clave de recuperación de BitLocker del dispositivo, almacenándola en el objeto del equipo en AD. Consulta Guardar la clave de BitLocker para obtener más información.
- Sincronizar el reloj del sistema con el controlador de dominio para la comunicación cifrada

Surface Hub no admite la aplicación de directivas de grupo o certificados desde el controlador de dominio.

> **NOTE**
> Si el Surface Hub pierde confianza en el dominio (por ejemplo, si se quita el Surface Hub del dominio cuando esté unido a este), no podrás autenticarte en el dispositivo ni abrir Configuración. Si decides quitar la relación de confianza entre el Surface Hub y tu dominio, restablece el dispositivo en primer lugar.

Azure AD unirse al dispositivo

Puede Azure Active Directory (Azure AD) unirse a la Surface Hub para permitir que los profesionales de TI de su inquilino Azure AD configurar la configuración. Durante la primera ejecución, elige usar Microsoft Azure Active Directory. Deberás proporcionar las credenciales que se pueden unir al inquilino de Azure AD de tu elección. Después de unirte a Azure AD correctamente, se concederán los derechos de administrador a las personas adecuadas en el dispositivo.

De manera predeterminada, se concederán derechos de administrador a todos los **administradores globales** en un Surface Hub unido a Azure AD. Con **Azure AD Premium** o **Enterprise Mobility Suite (EMS)**, puedes agregar administradores adicionales:

1. En el portal de Azure clásico, haz clic en **Active Directory** y, a continuación, haz clic en el nombre del directorio de la organización.
2. En la página **Configurar**, en **Dispositivos** > **Administradores adicionales en los dispositivos unidos a Azure AD**, haz clic en **Seleccionados**.
3. Haz clic en **Agregar** y selecciona los usuarios que quieres agregar como administradores en tu Surface Hub y en otros dispositivos unidos a Azure AD.
4. Cuando hayas terminado, haz clic en el botón de marca de verificación para guardar el cambio.

¿Qué sucede al unir el Surface Hub a Azure AD?

Los Surface Hubs usan la unión a Azure AD para:

- Conceder derechos de administrador a los usuarios adecuados en el inquilino de Azure AD.
- Copia de seguridad de la clave de recuperación de BitLocker del dispositivo, almacenándola en la cuenta que se usó para unir el dispositivo a Azure AD. Consulta Guardar la clave de BitLocker para obtener más información.

Inscripción automática a través Azure Active Directory unirse

Surface Hub ahora admite la capacidad de inscribirse automáticamente en Intune uniendo el dispositivo a Azure Active Directory.

Para obtener más información, vea Enable Windows 10 automatic enrollment.

¿Cuál debo elegir?

Si tu organización usa AD o Azure AD, te recomendamos que te unas a un dominio o a Azure AD, principalmente por motivos de seguridad. Las personas podrán autenticarse y desbloquear Configuración con sus propias credenciales y se pueden mover dentro o fuera de los grupos de seguridad asociados a tu dominio.

OPCIÓN	REQUISITOS	¿QUÉ CREDENCIALES SE PUEDEN USAR PARA ACCEDER A LA APLICACIÓN CONFIGURACIÓN?
Crear una cuenta de administrador local	Ninguna	El nombre de usuario y contraseña especificados durante la primera ejecución
Unión a un dominio de Active Directory (AD)	Tu organización usa AD	Cualquier usuario de AD de un grupo de seguridad específico de tu dominio

OPCIÓN	REQUISITOS	¿QUÉ CREDENCIALES SE PUEDEN USAR PARA ACCEDER A LA APLICACIÓN CONFIGURACIÓN?
Unir el dispositivo a Azure Active Directory (Azure AD)	Tu organización usa Azure AD Basic	Solo los administradores globales
	Tu organización usa Azure AD Premium o Enterprise Mobility Suite (EMS)	Los administradores globales y los administradores adicionales

Configurar cuentas de administración no globales en Azure AD dispositivos unidos

Para Surface Hub v1 y Surface Hub dispositivos 2S unidos a Azure AD, Windows 10 Team 2020 Update te permite limitar los permisos de administrador a la administración de la aplicación Configuración en Surface Hub. Esto le permite tener en cuenta los permisos de administración Surface Hub y evitar el acceso de administrador potencialmente no deseado a un dominio Azure AD usuario. Para obtener más información, vea Configure non Global admin accounts on Surface Hub.

Crear paquetes de aprovisionamiento para Surface Hub

12/01/2022 • 13 minutes to read

Los paquetes de aprovisionamiento te permiten automatizar la implementación de características clave, lo que ayuda a ofrecer una experiencia coherente en todos los Surface Hubs de tu organización. Con Windows Configuration Designer (WCD) en un equipo independiente, puede completar las siguientes tareas:

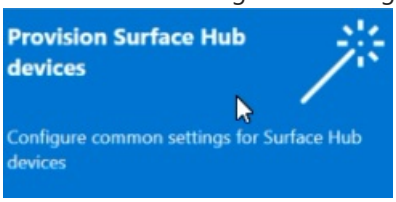
- Inscribirse en Active Directory o Azure Active Directory
- Crear una cuenta de administrador de dispositivos
- Agregar aplicaciones y certificados
- Definir la configuración de proxy
- Agregar un archivo de configuración de Surface Hub
- Configurar la configuración del proveedor de servicios de configuración (CSP)

Introducción

1. En un equipo independiente que ejecute Windows 10, instale Windows Configuration Designer desde el Microsoft Store.
2. Selecciona **Aprovisionar Surface Hub dispositivos para** configurar opciones comunes mediante un asistente. O bien, seleccione Aprovisionamiento avanzado para ver y configurar todas las opciones posibles.
3. Cree el paquete de aprovisionamiento y guárdelo en una unidad USB.
4. Implemente el paquete en su Surface Hub durante la instalación de la primera ejecución o a través de la Configuración aplicación. Para obtener más información, vea Create a provisioning package for Windows 10.

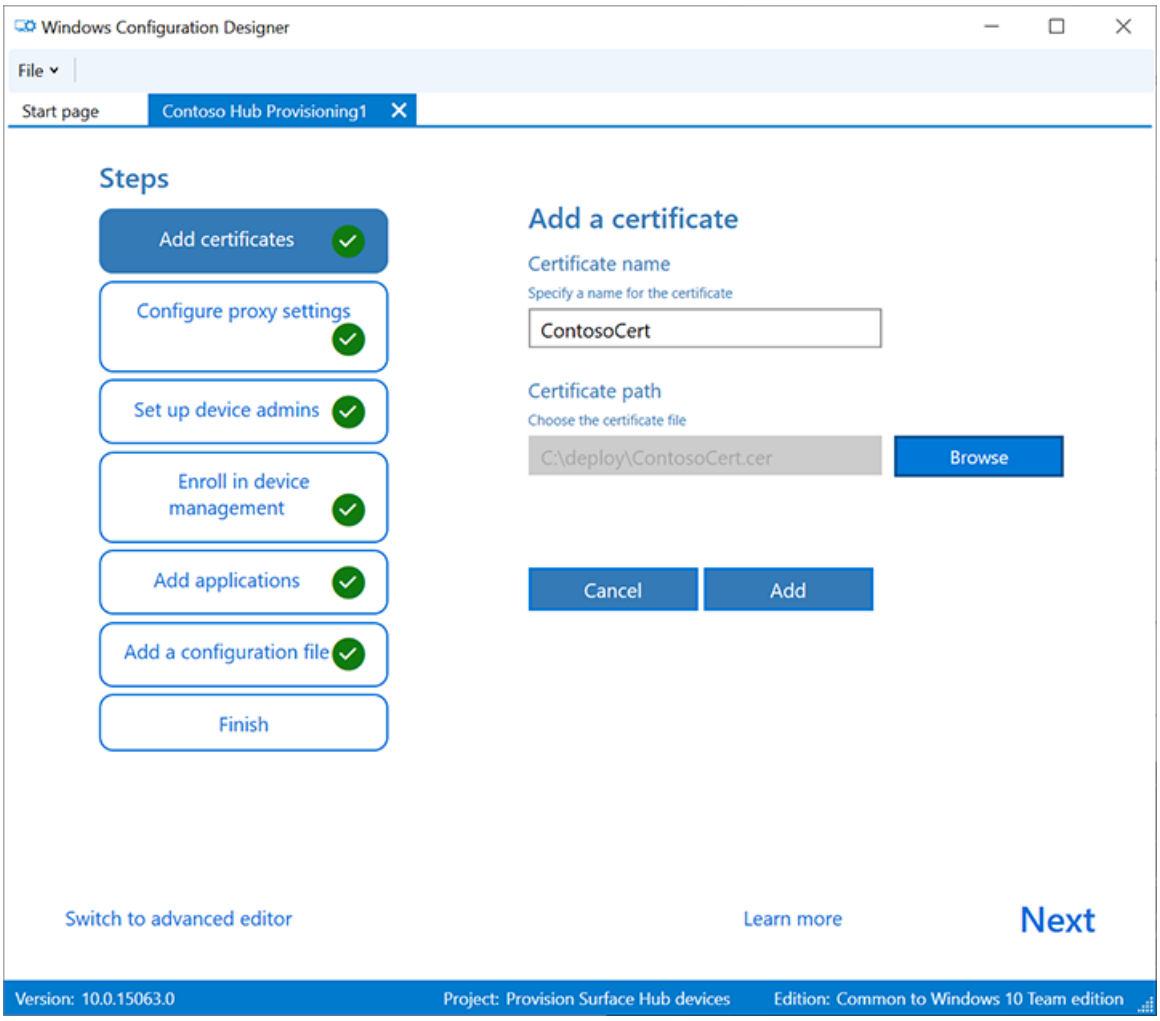
Usar Surface Hub de aprovisionamiento

1. Abra Windows Configuration Designer y seleccione **Aprovisionar Surface Hub dispositivos**.



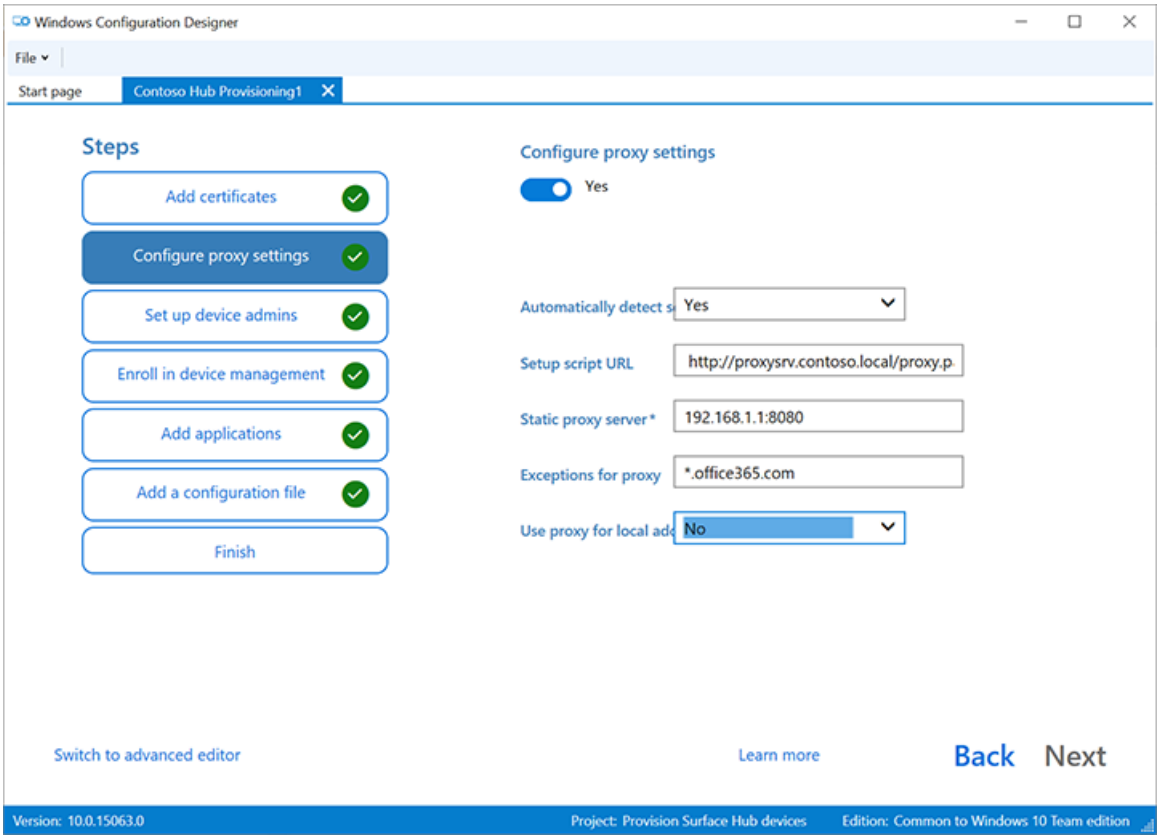
2. Asigne un nombre al proyecto y seleccione **Siguiente**.

Agregar certificados



Para aprovisionar el dispositivo con un certificado, **seleccione Agregar un certificado**. Escriba un nombre para el certificado y, a continuación, busque para seleccionar el certificado que se va a usar. Para obtener opciones avanzadas de aprovisionamiento, consulte la sección siguiente Agregar un certificado al paquete.

Definir la configuración de proxy



1. Alterna **Sí** o **No** para la configuración de proxy. De forma predeterminada, Surface Hub automáticamente detecta la configuración de proxy. Sin embargo, si anteriormente tu infraestructura requería el uso de un servidor proxy y ahora ha cambiado y ya no lo requiere, puedes usar un paquete de aprovisionamiento para revertir los dispositivos Surface Hub a la configuración predeterminada seleccionando **Sí** y **Detectar la configuración automáticamente**.

2. Si alterna **Sí**, puede seleccionar para detectar automáticamente la configuración de proxy o configurar manualmente la configuración especificando una de las siguientes opciones:

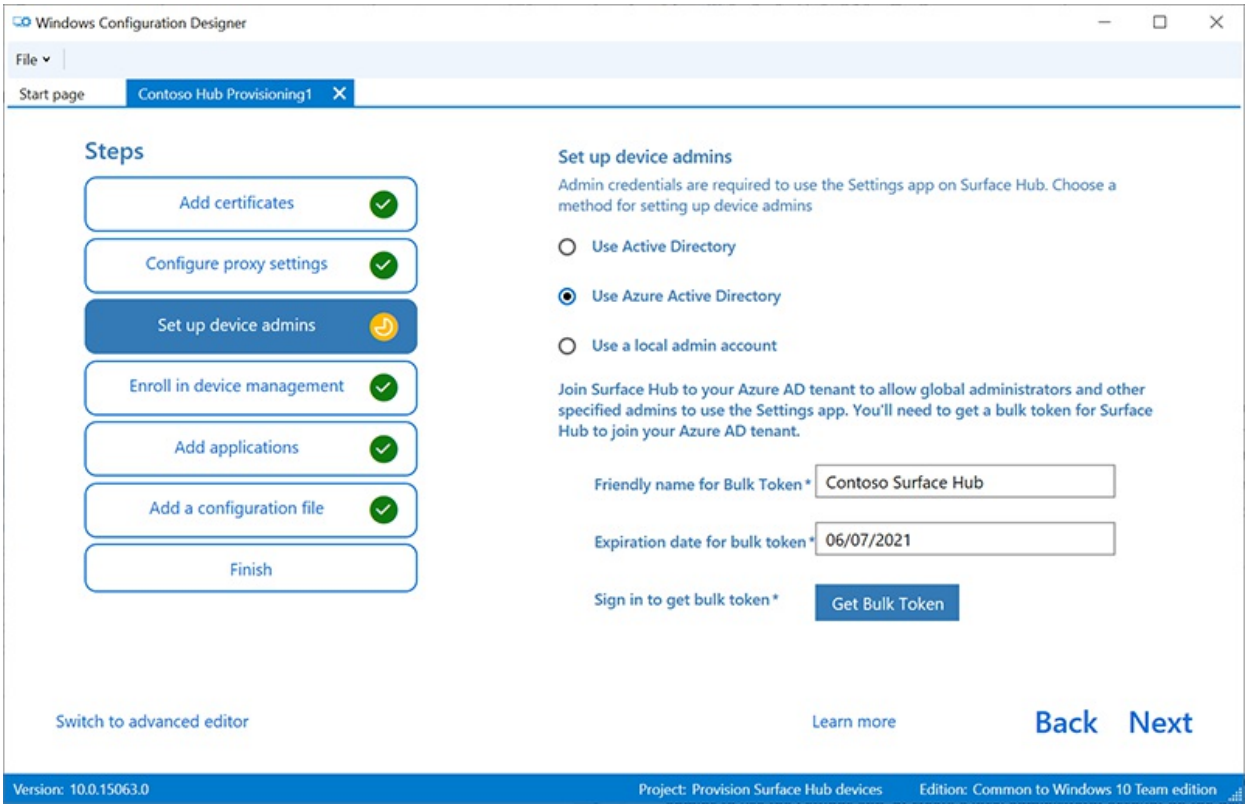
   - Dirección URL de un script de instalación.
   - Una dirección de servidor proxy estático e información de puerto.

3. Si desea usar un script de instalación o un servidor proxy, desactive **Detectar automáticamente la configuración**. Puede usar un script de instalación *o un* servidor proxy, no ambos.

4. Escriba excepciones (direcciones a las Surface Hub deben conectarse directamente sin usar el servidor proxy). **Ejemplo:** *.office365.com

5. Identificar si se va a usar el servidor proxy para las direcciones locales.

Configurar administradores de dispositivos



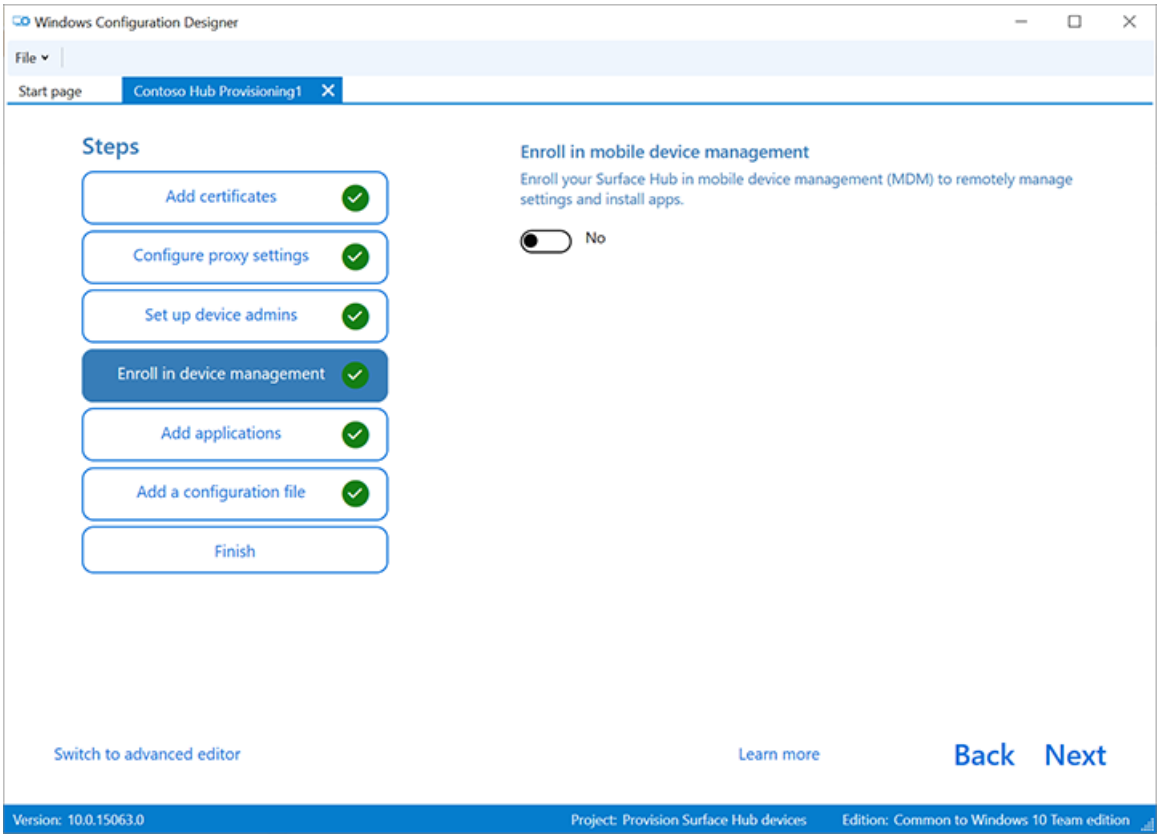
Puedes inscribir el dispositivo en Active Directory y especificar un grupo de seguridad para que use la aplicación Configuración, inscribirlo en Azure Active Directory para permitir que los administradores globales usen la aplicación Configuración o crear una cuenta de administrador local en el dispositivo.

1. Para inscribir el dispositivo en Active Directory, escribe las credenciales de una cuenta de usuario con privilegios mínimos para unir el equipo al dominio y especifica que el grupo de seguridad tenga credenciales de administrador en Surface Hub. Si aplica el paquete a un Surface Hub que se ha restablecido, puede usar la misma cuenta de dominio siempre que sea la misma cuenta la que configure el Surface Hub inicialmente. De lo contrario, se tiene que usar una cuenta de dominio diferente en el paquete de aprovisionamiento.
2. Antes de usar Windows Configuration Designer para configurar la inscripción masiva de Azure AD, planee laimplementación de la combinación de Azure AD . La opción **Número máximo de dispositivos por usuario** del inquilino de Azure AD determina cuántas veces se puede usar el token masivo que se obtiene en el asistente.

3. Para inscribir el dispositivo en Azure AD, selecciona esa opción y escribe un nombre descriptivo para el token masivo que obtendrás mediante el asistente. Establece una fecha de expiración del token (el máximo es de 30 días a partir de la fecha de obtención del token). Seleccione **Obtener token masivo**. En la ventana **Vamos a iniciar sesión**, escribe una cuenta que tenga permisos para unir un dispositivo a AzureAD y luego la contraseña. Seleccione **Aceptar** para conceder a Windows Configuration Designer los permisos necesarios.
4. Para crear una cuenta de administrador local, selecciona esa opción y escribe un nombre de usuario y una contraseña.

> **IMPORTANT**
>
> Si creas una cuenta local en el paquete de aprovisionamiento, debes cambiar la contraseña mediante la aplicación **Configuración** cada 42 días. Si la contraseña no se cambia en ese período, es posible que la cuenta se bloquee y no se pueda iniciar sesión.

Inscribirse en un proveedor MDM de terceros

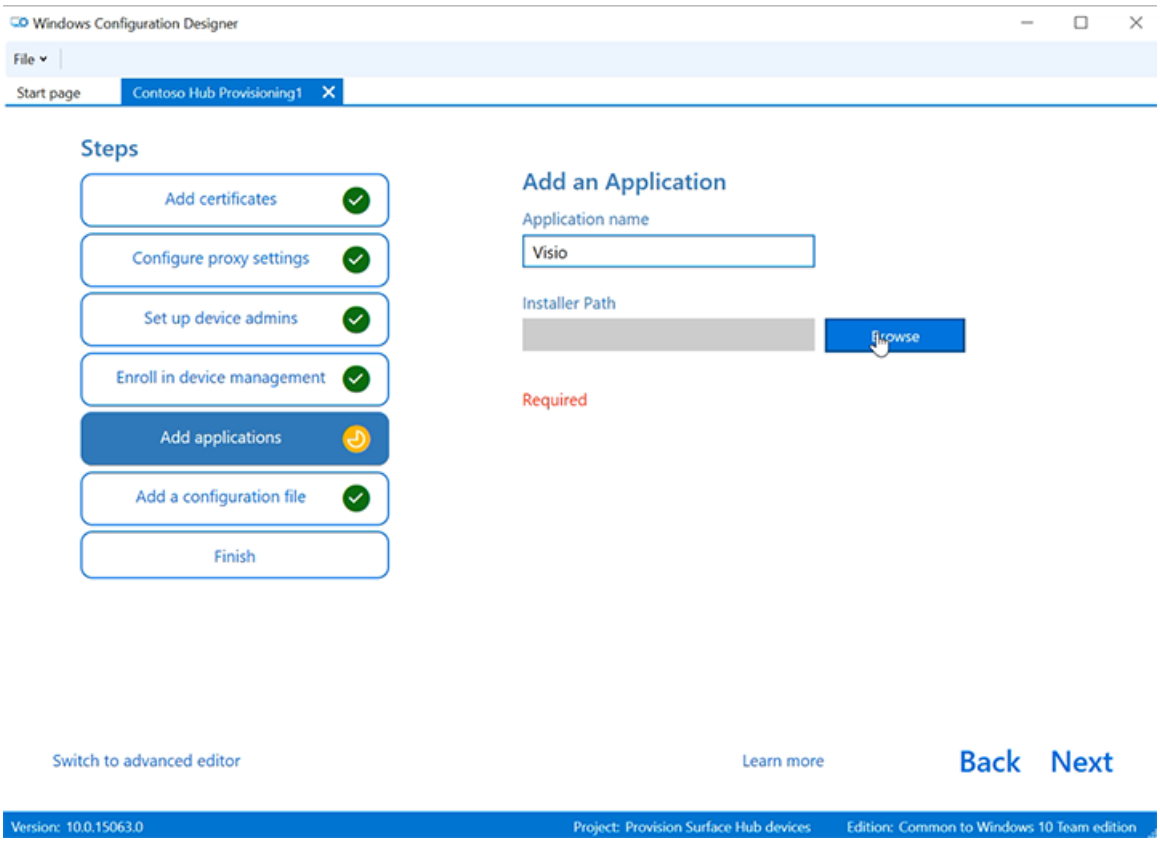


Si usas un proveedor de administración de dispositivos móviles (MDM) de terceros, puedes usar esta sección para inscribir Surface Hub. Para inscribirse en Intune, configure primero la combinación de Azure AD, tal como se describe en la sección anterior, y siga las instrucciones de la siguiente documentación de Intune: Configurar la inscripción automática para dispositivos Windows 10.

1. Alterna **Sí** o **No para** la inscripción en MDM de terceros.
2. Si alterna **Sí**, proporcione una cuenta de servicio y una contraseña o huella digital de certificado que esté autorizada para inscribir el dispositivo y especificar el tipo de autenticación.
3. Si el proveedor mdm lo requiere, escribe las direcciones URL del servicio de detección, el servicio de inscripción y el servicio de directivas.

Para obtener más información, consulta Administrar Surface Hub con un proveedor mdm.

Agregar aplicaciones



Puedes instalar varias aplicaciones para la Plataforma universal de Windows (UWP) en un paquete de aprovisionamiento. Para obtener más información, consulta Aprovisionar equipos con aplicaciones.

> **NOTE**
> Aunque Windows de configuración te permite agregar una aplicación clásica de Win32 a un paquete de aprovisionamiento, Surface Hub solo acepta aplicaciones para UWP. Si incluyes una aplicación Win32 clásica, el aprovisionamiento fallará.

Agregar un archivo de configuración

Además de este paquete de aprovisionamiento, puedes usar un archivo de configuración Surface Hub para facilitar aún más la configuración de los dispositivos. Un archivo de configuración de Surface Hub contiene una lista de cuentas de dispositivo para conectarse a Exchange, Microsoft Teams o Skype Empresarial, así como "nombres descriptivos" para la proyección inalámbrica.

Para crear un archivo Surface Hub de configuración:

1. Abra Microsoft Excel (u otro editor de .csv), cree un archivo .csv denominado *SurfaceHubConfiguration.csv*.
2. Escribe una lista de cuentas de dispositivo y nombres descriptivos en este formato:

```
<DeviceAccountName>,<DeviceAccountPassword>,<FriendlyName>
```

> **NOTE**
> El archivo de configuración no debe contener encabezados de columna. Cuando se incluye en un paquete de aprovisionamiento aplicado a Surface Hub, puedes seleccionar la cuenta y el nombre descriptivo del dispositivo desde el archivo. Para crear el archivo .csv, use un formato de dirección UPN (rainier@contoso.com) o un formato de nombre de inicio de sesión de nivel inferior (contoso\rainier).

rainier@contoso.com,password,Rainier Surface Hub

3. Guarde el archivo en la carpeta del proyecto y cópielo en la clave USB con el paquete de aprovisionamiento.

> **NOTE**
> El archivo de configuración solo se puede aplicar durante la instalación de la primera ejecución.

Paquete de aprovisionamiento de protección de contraseñas

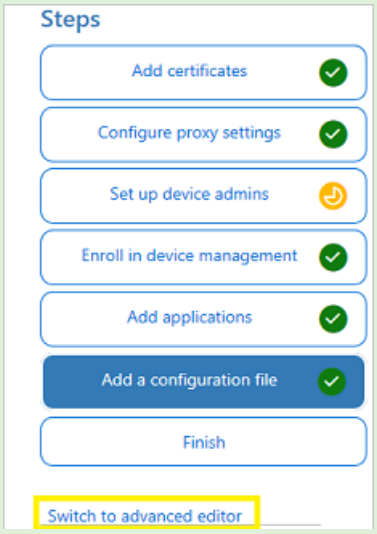
Si eliges usar una contraseña, deberás escribirla cada vez que apliques el paquete de aprovisionamiento a un dispositivo.

Asistente para aprovisionamiento completo

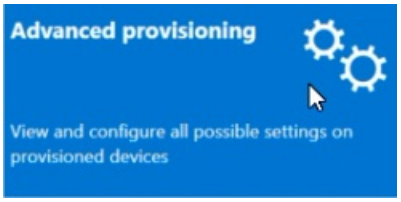
Si solo necesita configurar opciones comunes, seleccione **Finalizar**crear y > **** vaya a la sección Compilar el paquete. O bien, siga configurando la configuración cambiando al aprovisionamiento avanzado.

Usar aprovisionamiento avanzado

> **TIP**
> Usa el asistente para crear un paquete con la configuración común y después usa el editor avanzado para agregar otras configuraciones.

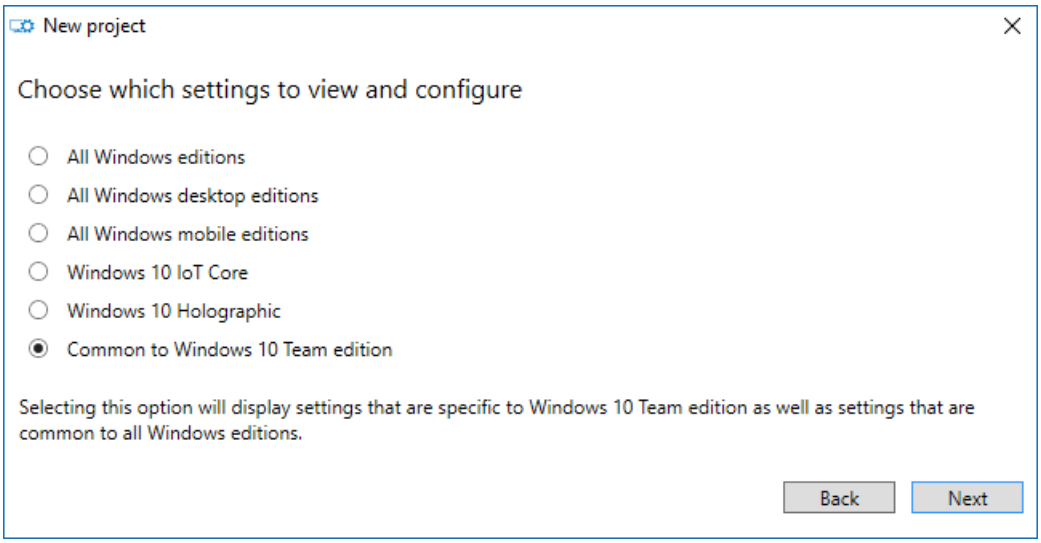


1. Si continúa en la sección anterior, seleccione **Cambiar al editor** avanzado de lo **contrario, abra Windows Diseñador** de configuraciones y seleccione **Aprovisionamiento avanzado**.

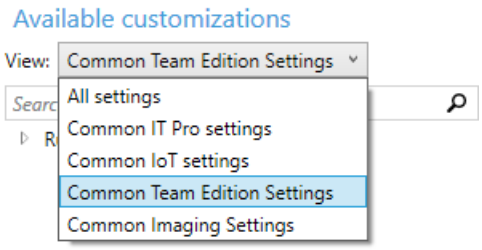


2. Asigne un nombre al proyecto y seleccione **Siguiente**.

3. Seleccione **Común para Windows 10 Team**, seleccione **Siguiente**y, a continuación, seleccione **Finalizar**.



4. En el proyecto, en **Personalizaciones disponibles,** seleccione **Configuración común del equipo**.



Agregar un certificado al paquete

Puedes usar paquetes de aprovisionamiento para instalar certificados que permitirán que el dispositivo se autentique en MicrosoftExchange.

> **NOTE**
> Los paquetes de aprovisionamiento solo pueden instalar certificados en el almacén de dispositivo (máquina local), pero no en el almacén del usuario. Si su organización requiere que los certificados se instalen en el almacén de usuarios, use la aplicación Central **Configuración: Actualizar**& certificados de seguridad > **** > **importar certificado**. Como alternativa, puedes usar directivas **MDM** para implementar certificados en el almacén de dispositivos o en el almacén de usuarios.

> **TIP**
> La **sección ClientCertificates** es para los archivos .pfx con una clave privada; los archivos .cer para las CA raíz deben colocarse en la sección **RootCertificates** y para las CA intermedias en la **sección CACertificates.**

1. En **Windows Configuration Designer** > **Personalizaciones** disponibles, vaya a **Configuración**de tiempo de ejecución > **Certificados** > **ClientCertificates**.
2. Escriba una etiqueta para **CertificateName** y, a continuación, **seleccione Agregar**.
3. Escribe el valor **CertificatePassword**.
4. Para el valor **CertificatePath**, examina y selecciona el certificado.
5. Establece el elemento **ExportCertificate** en **False**.
6. Para **KeyLocation**, selecciona **Software solo**.

Agregar una aplicación para UWP al paquete

Para agregar una aplicación para UWP a un paquete de aprovisionamiento, necesitarás el paquete de la aplicación (archivos .appx o .appxbundle) y los archivos de dependencia. Si adquiriste la aplicación en la

Microsoft Store para Empresas, también necesitarás la licencia de la aplicación *sin codificar*. Consulta Distribuir aplicaciones sin conexión para conocer cómo descargar estos elementos de la Microsoft Store para Empresas.

Para agregar una aplicación para UWP:

1. En el panel **Personalizaciones disponibles**, ve a **Configuración de tiempo de ejecución** > **UniversalAppInstall** > **DeviceContextApp**.
2. Escriba un **PackageFamilyName** para la aplicación y, a continuación, **seleccione Agregar**. Por motivos de coherencia, usa el nombre de familia de paquete de la aplicación. Si adquiriste la aplicación en la Microsoft Store para Empresas, puedes encontrar el nombre de familia de paquete en la licencia de la aplicación. Abra el archivo de licencia con un editor de texto y use el valor entre las etiquetas PFM.
3. Para **ApplicationFile,** seleccione **Examinar** para buscar y seleccionar la aplicación de destino (.appx o .appxbundle).
4. Para **DependencyAppxFiles,** seleccione **Examinar** para buscar y agregar cualquier dependencia para la aplicación. Para Surface Hub, solo necesitas versiones x64 de estas dependencias.

Si adquiriste la aplicación a Microsoft Store para Empresas, deberás agregar la licencia de la aplicación al paquete de aprovisionamiento.

Para agregar una licencia de aplicación:

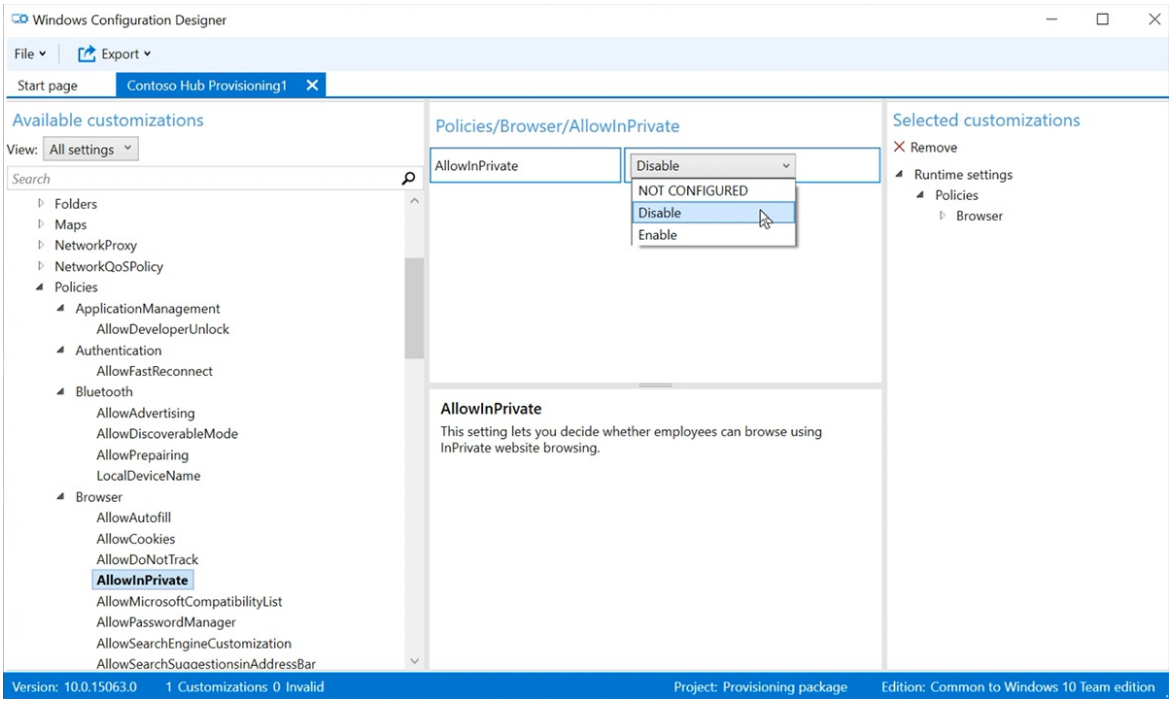
1. Haz una copia de la licencia de la aplicación y cámbiale el nombre para usar una extensión **.ms-windows-store-license**. Por ejemplo, cambie el nombre de "example.xml" a "example.ms-windows-store-license".
2. En Windows Configuration Designer, ve a **Available customizations** > **Runtime settings** > **UniversalAppInstall** > **DeviceContextAppLicense**.
3. Escriba un **LicenseProductId** y, a continuación, **seleccione Agregar**. Por motivos de coherencia, usa el identificador de licencia de aplicación de la licencia de la aplicación. Abre el archivo de licencia con un editor de texto. A continuación, en **la etiqueta License,** use el valor del **atributo LicenseID.**
4. Selecciona el nuevo nodo **LicenseProductId**. Para **LicenseInstall,** seleccione **Examinar** para buscar y seleccionar el archivo de licencia cuyo nombre ha cambiado (example.ms-windows-store-license).

Agregar una directiva al paquete

Surface Hub admite un subconjunto de directivas incluidas en el Proveedor de servicios de configuración de directivas. Algunas de estas directivas se pueden configurar con Windows de configuración.

Para agregar directivas csp:

1. Ve a **Personalizaciones disponibles Configuración de** > **tiempo de ejecución** > **Directivas**.
2. Seleccione el componente que desea administrar y configurar la configuración de directiva según corresponda. Por ejemplo, para impedir que los empleados utilicen la exploración del sitio web de InPrivate en Surface Hub, seleccione **AllowInPrivate** y, a continuación, **seleccione Deshabilitar**.



Agregar valores de configuración de Surface Hub al paquete

Puedes agregar valores de configuración del Proveedor de servicios de configuración de SurfaceHub al paquete de aprovisionamiento.

1. Vaya a **Personalizaciones disponibles** > **Common Team Edition Configuración**.
2. Seleccione el componente que desea administrar y configurar la configuración de directiva según corresponda.
3. Cuando haya terminado de configurar el paquete de aprovisionamiento, seleccione **Guardar** > **archivo**.
4. Lea la advertencia de que los archivos del proyecto pueden contener información confidencial y seleccione **Aceptar**

Crear el paquete

Cuando compilas un paquete de aprovisionamiento, puedes incluir información confidencial en los archivos de proyecto y en el archivo del paquete de aprovisionamiento (.ppkg). Aunque tienes la posibilidad de cifrar el archivo .ppkg, los archivos de proyecto no se cifran. Almacene los archivos del proyecto en una ubicación segura o elimine si ya no es necesario.

1. Abra **Windows paquete de aprovisionamiento de exportación del Diseñador**de > **** > **configuraciones**.
2. Cambiar **propietario a** administrador de **TI.**
3. Establece un valor para **Versión del paquete** y luego selecciona **Siguiente**.

> **TIP**
> Al establecer el propietario en Administrador de TI, se asegura de que la configuración del paquete mantenga las "propiedades de prioridad" adecuadas y permanezca en vigor en Surface Hub si otros paquetes de aprovisionamiento se aplican posteriormente desde otros orígenes.

> **TIP**
> Puede modificar los paquetes existentes y cambiar el número de versión para actualizar los paquetes aplicados anteriormente.

4. Opcional: puede elegir cifrar el paquete y habilitar la firma del paquete:

    a. Seleccione **Cifrar paquete y,** a continuación, escriba una contraseña.
    b. Seleccione **Firmar paquete** > **Examinar** y elija el certificado según corresponda.

    > **IMPORTANT**
    > Se recomienda incluir un certificado de aprovisionamiento de confianza en el paquete de aprovisionamiento. Cuando el paquete se aplica a un dispositivo, el certificado se agrega al almacén del sistema, lo que permite que los paquetes posteriores se apliquen de forma silenciosa.

5. Seleccione **Siguiente** para especificar la ubicación de salida. De forma predeterminada, el Diseñador de configuraciones de Windows usa la carpeta de proyecto como la ubicación de salida. O seleccione **Examinar para** cambiar la ubicación de salida predeterminada. Selecciona **Siguiente**.

6. Seleccione **Compilar** para empezar a compilar el paquete. La información del proyecto se muestra en la página de compilación.

7. Si se produce un error en la compilación, aparecerá un mensaje de error con un vínculo a la carpeta del proyecto. Revise los registros para diagnosticar el error y vuelva a compilar el paquete.

8. Si la compilación se realiza correctamente, se muestra el nombre del paquete de aprovisionamiento, el directorio de salida y el directorio del proyecto. Seleccione **Finalizar** para cerrar el asistente y volver a la página Personalizaciones.

9. Seleccione **la ubicación de** salida para ir a la ubicación del paquete. Copia el archivo .ppkg a una unidad flash USB.

Aplicar un paquete de aprovisionamiento a un dispositivo Surface Hub

Hay dos formas de implementar paquetes de aprovisionamiento en un Surface Hub:

- Ejecute el programa de instalación en primer lugar. Puedes aplicar un paquete de aprovisionamiento para personalizar varias opciones, incluidas la configuración Wi-Fi, la configuración de proxy, los detalles de la cuenta del dispositivo, la unión a Azure AD y la configuración relacionada.
- Configuración aplicación. Después de ejecutar el programa de instalación por primera vez, puedes aplicar un paquete de aprovisionamiento a través Configuración aplicación.

Aplicar un paquete de aprovisionamiento durante la primera ejecución

1. Cuando se activa el Surface Hub por primera vez, el programa de primera ejecución muestra **la página Hi there**. Asegúrate de que las opciones de configuración se hayan configurado correctamente antes de continuar.

2. Inserta la unidad flash USB que contiene el archivo .ppkg en el Surface Hub. Si el paquete está en el directorio raíz de la unidad, el programa de primera ejecución lo reconocerá y preguntará si quieres configurar el dispositivo. Selecciona **Configurar**.

3. La pantalla siguiente te pide que selecciones un origen de aprovisionamiento. Selecciona **Medios extraíbles** y pulsa **Siguiente**.

4. Selecciona el paquete de aprovisionamiento (*.ppkg) que quieras aplicar y pulsa **Siguiente**. Ten en cuenta que solo puedes instalar un paquete durante la primera ejecución.

5. El programa de primera ejecución mostrará un resumen de los cambios que va a aplicar el paquete de aprovisionamiento. Selecciona **Sí, agrégalo**.

6. Si un archivo de configuración se incluye en el directorio raíz de la unidad flash USB, verás **Seleccionar una configuración**. Se mostrará la primera cuenta de dispositivo en el archivo de configuración con un resumen de la información de la cuenta que se aplicará a Surface Hub.

7. En **Seleccionar una configuración,** seleccione el nombre del dispositivo que desea aplicar y, a continuación, **seleccione Siguiente**.

La configuración del paquete de aprovisionamiento se aplicará al dispositivo y se completará la configuración rápida. Una vez reiniciado el dispositivo, puedes quitar la unidad flash USB.

Aplicar un paquete de aprovisionamiento mediante Configuración aplicación

1. Inserta la unidad flash USB que contiene el archivo .ppkg en el Surface Hub.
2. Desde Surface Hub, inicie **Configuración** y escriba las credenciales de administrador cuando se le pida.
3. Navega hasta **Surface Hub** > **Administración de dispositivos**. En **Paquetes de aprovisionamiento, seleccione Agregar o quitar un paquete de aprovisionamiento**Agregar un > **paquete**.
4. Elige el paquete de aprovisionamiento y selecciona **Agregar**. Si se le pide, vuelva a escribir sus credenciales de administrador.
5. Verá un resumen de los cambios que se aplicarán. Selecciona **Sí, agrégalo**.

Obtén más información

- Descargar Windows de configuración
- Crear un paquete de aprovisionamiento para Windows10
- Administrar Surface Hub con un proveedor MDM

Crear y probar una cuenta del dispositivo (Surface Hub)

12/01/2022 • 4 minutes to read

La creación de una cuenta de dispositivo Surface Hub (también conocida como cuenta de recurso/buzón de sala) permite al Surface Hub recibir, aprobar o rechazar solicitudes de reunión y unirse a reuniones.

Una vez que la cuenta del dispositivo se aprovisiona en un Surface Hub, los usuarios pueden agregar esta cuenta a una invitación a una reunión del mismo modo que invitarían a una sala de conferencias.

Puedes configurar la cuenta del dispositivo durante la configuración de la experiencia de salida (OOBE). Si es necesario, también puede cambiarlo más adelante **en Configuración** > **Surface Hub** > **Accounts**.

Introducción a la configuración

Esta tabla explica los pasos principales y las decisiones de configuración cuando se crea una cuenta del dispositivo.

PASO	DESCRIPCIÓN	PROPÓSITO
1	Crear un buzón de sala habilitado para inicio de sesión (Exchange Online o Exchange Server 2016 y versiones posteriores)	Este tipo de buzón permite al dispositivo mantener un calendario de reuniones, recibir solicitudes de reunión y enviar correo. Debe estar habilitado para el inicio de sesión para poder usarse con un Surface Hub.
2	Configurar las propiedades de buzón de correo	El buzón de correo debe estar configurado con las propiedades correctas para obtener la mejor experiencia de reunión en Surface Hub. Para obtener más información acerca de las propiedades del buzón de correo, consulta Propiedades del buzón.
3	Asegúrese de Exchange web Services (EWS) está habilitado y de que la autenticación multifactor (MFA) está deshabilitada	El Surface Hub usa EWS para sincronizar su calendario. Si no permite EWS en el entorno de forma predeterminada, el buzón de concentradores tendría que tenerla habilitada explícitamente. Como el Surface Hub inicia sesión Exchange en segundo plano sin la interacción del usuario, no puede responder a ningún mensaje interactivo, como MFA. La cuenta de dispositivo que cree debe excluirse de dichos requisitos de autenticación. De lo contrario, Surface Hub no podrá sincronizar el correo ni la información de calendario.

PASO	DESCRIPCIÓN	PROPÓSITO
4	Habilitar la cuenta para Teams o Skype Empresarial (Skype Empresarial Server 2015 y versiones posteriores)	Skype Empresarial o Teams deben habilitarse para usar características de conferencia como videollamadas y uso compartido de pantalla. Para obtener más información sobre las licencias que Teams, vea Teams Sala de reuniones licensing and Teams service description. Las aplicaciones Teams y SfB de la Surface Hub no son compatibles con las directivas de acceso condicional de Azure AD que requieren información del dispositivo (por ejemplo, cumplimiento). La cuenta de dispositivo que cree debe excluirse de dichas directivas de CA. De lo contrario, Surface Hub no puede usar ninguna función de conferencia.
5	(Opcional) Deshabilitar la caducidad de contraseña	Para simplificar la administración, puedes desactivar la caducidad de contraseña para la cuenta del dispositivo y permitir que Surface Hub rote automáticamente la contraseña de la cuenta del dispositivo. Para obtener más información acerca de la administración de contraseñas, consulta Administración de contraseñas.
6	(Opcional) Configurar Exchange directivas para permitir ActiveSync	Con determinadas implementaciones Exchange Server & de Active Directory locales, ActiveSync se usará para sincronizar el correo de la cuenta del dispositivo y la información del calendario. Para obtener más información acerca de las directivas que se configurarán, vea Directivas de ActiveSync para Surface Hub cuentas.

NOTE

La Surface Hub de dispositivo no admite proveedores de identidades federados (IDP) de terceros y debe autenticarse a través de Active Directory o Azure Active Directory.

Pasos detallados de la configuración

Se recomienda configurar las cuentas Surface Hub dispositivo mediante el uso de Windows PowerShell. Microsoft proporciona SkypeRoomProvisioningScript.ps1, un script que ayudará a crear nuevas cuentas de recursos o validar cuentas de recursos existentes que tenga para ayudarle a convertirlos en cuentas de dispositivo Surface Hub compatibles. Si lo prefiere, puede elegir una opción de la tabla siguiente y seguir los pasos detallados de PowerShell en función de la implementación de la organización.

IMPLEMENTACIÓN DE LA ORGANIZACIÓN	DESCRIPCIÓN	FORMATO QUE SE USARÁ DURANTE SURFACE HUB INSTALACIÓN
Implementación en línea (Microsoft 365 o Office 365)	El entorno de la organización se implementa completamente en Microsoft 365 o Office 365.	nombreusuario@dominio.com
Implementación híbrida (Exchange local)	Su organización tiene una combinación de servicios, con Exchange Server local y Microsoft Teams en línea.	username@domain.com si la autenticación moderna híbrida está habilitada en Exchange, DOMAIN\username en caso contrario
Implementación híbrida (Exchange Online)	Su organización tiene una combinación de servicios, con Skype Empresarial Server local y Exchange Online.	username@domain.com si la autenticación moderna híbrida está habilitada en SfB, DOMAIN\username de lo contrario
Implementación local (bosque único)	Su organización tiene servidores que controla, donde Active Directory, Exchange y Skype Empresarial Server se hospedan en un entorno de bosque único.	DOMINIO\nombre de usuario
Implementación local (varios bosques)	Su organización tiene servidores que controla, donde Active Directory, Exchange y Skype Empresarial Server se hospedan en un entorno de varios bosques.	ACCOUNTFOREST\username

Verificación y prueba de cuentas

Hay dos métodos disponibles que puedes usar para validar y probar una cuenta Surface Hub dispositivo:SkypeRoomProvisioningScript.ps1y la aplicación Surface Hub de diagnóstico de hardware. El script de aprovisionamiento de cuenta puede validar una cuenta de dispositivo creada previamente con PowerShell desde el equipo. La aplicación Diagnóstico de hardware de Surface Hub se instala en Surface Hub y proporciona información detallada acerca de los errores de inicio de sesión y comunicación. Ambas son herramientas valiosas para probar las cuentas del dispositivo recién creadas y deben usarse para garantizar una óptima disponibilidad de las cuentas.

Propiedades de Microsoft Exchange (Surface Hub)

12/01/2022 • 2 minutes to read

Algunas propiedades de Microsoft Exchange de la cuenta del dispositivo se deben establecer en determinados valores para obtener la mejor experiencia de reunión en Microsoft Surface Hub. La siguiente tabla enumera varias propiedades de Exchange basadas en parámetros de cmdlet de PowerShell, su propósito y los valores en los que se deberían establecer.

PROPIEDAD	DESCRIPCIÓN	VALOR	IMPACTO
AutomateProcessing	El parámetro AutomateProcessing habilita o deshabilita el procesamiento de calendario en el buzón.	AutoAccept	El Surface Hub podrá aceptar o rechazar automáticamente las convocatorias de reunión según su disponibilidad.
AddOrganizerToSubject	El parámetro AddOrganizerToSubject especifica si el nombre del organizador de la reunión se usa como el asunto de la convocatoria de reunión.	$False	La pantalla de bienvenida no mostrará al organizador de la reunión dos veces (en lugar de mostrarlo tanto como el organizador como el asunto de la reunión).
AllowConflicts	El parámetro AllowConflicts especifica si se permiten convocatorias de reunión en conflicto.	$False	El Surface Hub rechazará las convocatorias de reunión que entren en conflicto con la hora de otra reunión.
DeleteComments	El parámetro DeleteComments especifica si se quita o se mantiene cualquier texto en el cuerpo del mensaje de las convocatorias de reunión entrantes.	$False	El cuerpo del mensaje de las reuniones se puede conservar y recuperar desde un Surface Hub si lo necesitas durante una reunión.
DeleteSubject	El parámetro DeleteSubject especifica si se debe quitar o mantener el asunto de las convocatorias de reunión entrantes.	$False	Los temas de las convocatorias de reunión se puede mostrar en el Surface Hub.

PROPIEDAD	DESCRIPCIÓN	VALOR	IMPACTO
RemovePrivateProperty	El parámetro RemovePrivateProperty especifica si se borra la marca privada para las convocatorias de reunión entrantes.	$False	Los temas de las reuniones privadas se mostrará como Privado en la pantalla de bienvenida.
AddAdditionalResponse	El parámetro AddAdditionalResponse especifica si se enviará información adicional desde el buzón de recursos al responder a las convocatorias de reunión.	$True	Cuando se envía una respuesta a una convocatoria de reunión, se proporcionará texto personalizado en la respuesta.
AdditionalResponse	El parámetro AdditionalResponse especifica la información adicional que se incluirá en las respuestas a las convocatorias de reunión. **Nota:** este texto no se enviará a menos que AddAdditionalResponse se establezca en $true.	Tu elección: la respuesta adicional se puede usar para indicar a los usuarios cómo usar un Surface Hub o guiarlos a los recursos.	Al añadir un mensaje de respuesta adicional se puede proporcionar a los usuarios una introducción sobre cómo pueden usar un Surface Hub en su reunión.

Aplicación de directivas de ActiveSync a las cuentas de dispositivo (Surface Hub)

12/01/2022 • 2 minutes to read

Los Surface Hub que usan cuentas de dispositivo **** de Active Directory (aprovisionadas en el concentrador en formato dominio\nombredeusuario) y los servicios de Exchange locales usan ActiveSync para sincronizar el correo y el calendario. Esto permite a los usuarios unirse e iniciar reuniones programadas desde Surface Hub, así como enviar por correo electrónico cualquier pizarra interactiva realizada durante la reunión.

Para que estas características funcionen, las directivas de ActiveSync de tu organización deben configurarse de la siguiente manera:

- No puede haber ninguna directiva global que bloquee la sincronización del buzón de recursos que está usando la cuenta del dispositivo de Surface Hub. Si hay una directiva de bloqueo de este tipo, debes agregar Surface Hub como dispositivo permitido.
- Debes establecer una directiva de buzón de dispositivo móvil donde la **PasswordEnabled** configuración esté establecida en False. Otras opciones de configuración de directiva de buzón de dispositivo móvil no son compatibles con el Surface Hub.

Permitir deviceid

La organización puede tener una directiva global que impida la sincronización de cuentas de dispositivos aprovisionadas en Surface Hubs. Para configurar esta propiedad, consulta Permitir id. de dispositivo para ActiveSync.

Configuración PasswordEnabled

La cuenta del dispositivo debe tener una directiva ActiveSync donde el atributo **PasswordEnabled** esté establecido en False o 0. Para configurar esta propiedad, consulta Creación de una directiva de Microsoft Exchange ActiveSync compatible con Surface Hub.

Configurar Microsoft Surface Hub

12/01/2022 • 2 minutes to read

Las instrucciones de configuración para Surface Hub incluyen una hoja de cálculo del programa de instalación y un tutorial sobre el programa de primera ejecución.

Antes de encender Microsoft Surface Hub por primera vez, asegúrate de haber completado la lista de comprobación al final de la sección Preparar el entorno para Surface Hub y de que se muestra la información en la hoja de cálculo del programa de instalación. Al encenderlo, el dispositivo te guiará a través de una serie de pantallas de instalación. Si no has configurado correctamente el entorno o no tienes la información necesaria, tendrás que realizar trabajo adicional después para asegurarte de que la configuración sea correcta.

En esta sección:

TEMA	DESCRIPCIÓN
Hoja de cálculo del programa de instalación	Cuando'terminado la configuración previa y está listo para iniciar la configuración de primera hora para su Surface Hub, asegúrese de tener toda la información que se muestra en esta sección.
Programa en primera ejecución	El término " primera ejecución " hace referencia a la serie de pasos que'recorren la primera vez que enciendes Surface Hub, y significa lo mismo que la " Configuración rápida " (OOBE). En esta sección te guiará por el proceso.

Hoja de cálculo del programa de instalación (Surface Hub)

12/01/2022 • 8 minutes to read

Cuando hayas terminado la preinstalación y estés preparado para iniciar la primera instalación de tu Microsoft Surface Hub, asegúrate de que tienes toda la información que se muestra en esta sección.

Debes rellenar una lista para cada Surface Hub que necesitas configurar, aunque cierta información se puede usar en todos los Surface Hubs, como la información de proxy o las credenciales de dominio. Parte de esta información puede no ser necesaria, en función de cómo hayas decidido configurar el dispositivo o según cómo esté configurado el entorno de la infraestructura de la organización.

Cuando haya terminado, revise Publicar lista de comprobación de implementación a continuación.

PROPIEDAD	ESTO SE USA PARA	EJEMPLO	OBTÉN MÁS INFORMACIÓN
Información de proxy	Si usa un proxy para el acceso a Internet o de red, debe proporcionar un script o información de servidor o puerto.	Script de proxy: http://contoso/proxy.pac O: Información de servidor y puerto: 10.10.10.100, puerto 80	Configurar el proxy mediante el paquete de aprovisionamiento.
Credenciales de red inalámbrica (nombre de usuario y contraseña)	Si conecta el dispositivo a Wi-Fi y la red inalámbrica requiere credenciales de usuario.	admin1@contoso.com, #MyPassw0rd	Administración de redes inalámbricas
UPN de la cuenta del dispositivo o Dominio\nombre de usuario y la contraseña de la cuenta del dispositivo	Este es el nombre principal de usuario (UPN) o el dominio\nombre de usuario y la contraseña de la cuenta del dispositivo. El correo, el calendario, Microsoft Teams y Skype Empresarial dependen de una cuenta de dispositivo compatible.	UPN: ConfRoom15@contoso.com, #Passw0rd1 O: Dominio y nombre de usuario: CONTOSO\ConfRoom15, #Passw0rd1	Crear y probar una cuenta de dispositivo
Propiedades del buzón	El buzón de correo debe estar configurado con las propiedades correctas para obtener la mejor experiencia de reunión en Surface Hub.	Vea Propiedades Exchange Microsoft	

PROPIEDAD	ESTO SE USA PARA	EJEMPLO	OBTÉN MÁS INFORMACIÓN
DIRECCIÓN URL de EWS para el buzón de la cuenta de dispositivo	Este es el servidor Exchange de la cuenta del dispositivo. El correo, el calendario, Microsoft Teams y Skype Empresarial dependen de una cuenta de dispositivo compatible. Para que el correo electrónico y el calendario funcionen, la cuenta del dispositivo debe tener un servidor Exchange válido. El dispositivo intentará encontrar esto automáticamente.	https://outlook.office365.com/EWS/exchange.asmx	Crear y probar una cuenta de dispositivo Propiedades de Microsoft Exchange
Dirección de Protocolo de inicio de sesión (SIP) de la cuenta del dispositivo	Esta es la dirección SIP de la cuenta del dispositivo. El correo, el calendario, Microsoft Teams y Skype Empresarial dependen de una cuenta de dispositivo compatible. Para que los equipos o Skype empresa funcionen, la cuenta del dispositivo debe tener una dirección SIP válida El dispositivo intentará encontrarlo automáticamente.	sip: ConfRoom15@contoso.com	
Contraseña de la cuenta de dispositivo	Para simplificar la administración, puedes deshabilitar la expiración de contraseña para la cuenta del dispositivo o permitir Surface Hub girar automáticamente la contraseña de la cuenta del dispositivo. **Nota:** Si agrega la cuenta en formato dominio\nombredeusuario, afilia el Concentrador a Active Directory local durante la instalación inicial. Si agrega la cuenta en username@domain.com, afilia el concentrador con Azure Active Directory durante la configuración inicial. De lo contrario, la rotación de contraseñas no funcionará.		Administración de contraseñas
Exchange Servicios web (EWS)	Habilitar EWS. Surface Hub usa EWS para sincronizar su calendario.		Autenticación moderna en Surface Hub

PROPIEDAD	ESTO SE USA PARA	EJEMPLO	OBTÉN MÁS INFORMACIÓN
Autenticación multifactor	Deshabilita la autenticación multifactor en la cuenta del dispositivo. Como el Surface Hub inicia sesión Exchange en segundo plano sin la interacción del usuario, no puede responder a ningún mensaje interactivo, como la autenticación multifactor.		
Detalles de inscripción de MDM	Si quieres inscribir manualmente el dispositivo en MDM, deberás tener credenciales de usuario válidas para el proveedor mdm y la dirección URL de inscripción. El dispositivo intentará encontrar la dirección URL de inscripción automáticamente.	manage.microsoft.com	Administrar Surface Hub con un proveedor MDM
Nombre descriptivo	El nombre descriptivo del dispositivo es el nombre de emisión que los usuarios verán cuando intenten conectarse de forma inalámbrica al Surface Hub. Este nombre se mostrará de forma destacada en la pantalla del Surface Hub. Se recomienda que el nombre descriptivo que elijas sea reconocible y único para que los usuarios puedan distinguir un Surface Hub de otro al intentar conectarse.	Sala de conferencias 15	Configuración por primera vez para Surface Hub
Nombre de dispositivo	El nombre del dispositivo es el nombre que se usará para unirse a un dominio y es la identidad que verás en el proveedor MDM si el dispositivo está inscrito en el MDM. El nombre del dispositivo que elijas no debe ser el mismo nombre que cualquier otro dispositivo del dominio de Active Directory (si decides unirte al dispositivo en el dominio). El dispositivo no puede unirse al dominio sin un nombre único.	confroom15	Configuración por primera vez para Surface Hub

PROPIEDAD	ESTO SE USA PARA	EJEMPLO	OBTÉN MÁS INFORMACIÓN
Modo de aplicación de Teams	- Modo 0: Skype Empresarial con Microsoft Teams funcionalidad para reuniones programadas. - Modo 1: Microsoft Teams con Skype Empresarial funcionalidad para reuniones programadas. - Modo 2: Microsoft Teams solo		Cambiar la plataforma de comunicaciones empresariales predeterminada

Afiliación de dispositivos

Usa la afiliación a dispositivos para administrar el acceso de los usuarios a Configuración aplicación en Surface Hub. Con el Windows 10 Team operativo (que se ejecuta en Surface Hub), solo los usuarios autorizados pueden ajustar la configuración con la Configuración aplicación. Dado que elegir la afiliación puede afectar a la disponibilidad de las características, planee correctamente para garantizar que los usuarios puedan acceder a las características según lo previsto.

> **NOTE**
> Solo puedes establecer la afiliación de dispositivos durante la configuración inicial de la experiencia de inicio de la caja (OOBE). Si necesitas restablecer la afiliación a dispositivos, tendrás que repetir la configuración de OOBE.

Si te unes a Azure AD

PROPIEDAD	ESTO SE USA PARA	EJEMPLO	OBTÉN MÁS INFORMACIÓN
Credenciales de usuario de inquilino de Azure AD (nombre de usuario y contraseña)	Si decide que los usuarios de la organización de Azure Active Directory (Azure AD) se conviertan en administradores en el dispositivo, deberá unirse a la Surface Hub a Azure AD. Para unirse a Azure AD, necesitará credenciales válidas para una cuenta en el inquilino.	admin1@contoso.com, #MyPassw0rd	Administración del grupo de administradores
Cuentas de administrador no globales	Para Surface Hub unidos a Azure AD, puede limitar los permisos de administración a la administración de la aplicación Configuración en Surface Hub. Esto le permite tener en cuenta los permisos de administración Surface Hub y evitar el acceso de administrador potencialmente no deseado a todo un dominio de Azure AD.		Configurar cuentas de administrador no globales en Surface Hub

Si se une a un dominio

PROPIEDAD	ESTO SE USA PARA	EJEMPLO
Dominio al que unirse	Este es el dominio al que debes unirte para que un grupo de seguridad de tu elección pueda ser administrador del dispositivo. Es posible que necesites el nombre de dominio completo (FQDN).	contoso (nombre corto) O contoso.corp.com (FQDN)
Credenciales de cuenta de dominio (nombre de usuario y contraseña)	No puedes unirte a un dominio a menos que proporciones las credenciales de cuenta suficientes para unirte al dominio. Una vez que proporciones un dominio al que unirte y las credenciales para unirte al dominio, un grupo de seguridad de tu elección podrá cambiar la configuración del dispositivo.	admin1, #MyPassw0rd
Alias del grupo de seguridad de administrador	Este es un grupo de seguridad de tu Active Directory (AD); todos los miembros de este grupo de seguridad pueden cambiar la configuración del dispositivo.	SurfaceHubAdmins

Si usa un administrador local

PROPIEDAD	ESTO SE USA PARA	EJEMPLO
Credenciales de cuenta de administrador local (nombre de usuario y contraseña)	Si no quieres unirte a un dominio de AD o a Azure AD, puedes crear una cuenta de administrador local en el dispositivo.	admin1, #MyPassw0rd

Si necesitas instalar certificados o aplicaciones

PROPIEDAD	ESTO SE USA PARA
Unidad USB	Si sabes antes de ejecutar por primera vez que quieres instalar certificados o aplicaciones universales, sigue los pasos de Crear paquetes de aprovisionamiento para Surface Hub. Los paquetes de aprovisionamiento se crearán en una unidad USB.

Lista de comprobación posterior a la implementación

COMPROBADO	RESPUESTA
Sincronización de cuentas de dispositivo	☐ Sí ☐ No
Clave de Bitlocker	☐ guardado en archivo (sin afiliación) ☐ guardado en Active Directory (afiliación a AD) ☐ guardado en Azure AD (afiliación a Azure AD)

COMPROBADO	RESPUESTA
Actualizaciones del sistema operativo del dispositivo	☐ completado
Windows Actualizaciones de la Tienda	☐ automático ☐ manual
Microsoft Teams reunión programada	☐ correo electrónico de confirmación recibido ☐ reunión aparece en la pantalla de inicio ☐ de unión con un solo toque ☐ puede unirse al audio ☐ puede unirse al vídeo ☐ puede compartir pantalla
Skype Empresarial reunión programada	☐ correo electrónico de confirmación recibido ☐ reunión aparece en la pantalla de inicio ☐ funciones de unión con un solo toque correctamente ☐ puede unirse al audio ☐ puede unirse al vídeo ☐ puede compartir pantalla ☐ puede enviar/recibir mensajería instantánea
Reunión programada cuando ya está invitada	☐ de reunión rechazada
Microsoft Teams reunión ad-hoc	☐ invitar a otros usuarios a trabajar ☐ puede unirse al audio ☐ puede unirse al vídeo ☐ puede compartir pantalla
Microsoft Whiteboard	☐ inicio desde la pantalla Inicio /Inicio ☐ iniciar desde Microsoft Teams
Llamada Teams/Skype entrante	☐ puede unirse al audio ☐ puede unirse al vídeo ☐ puede compartir pantalla ☐ puede enviar/recibir mi mi (solo Skype Empresarial)
Secuencias de vídeo en directo entrantes	☐ máximo 2 (Skype Empresarial) ☐ máximo 4 (Microsoft Teams)
Microsoft Teams Comportamiento del modo 0	☐ Skype Empresarial icono en la pantalla Inicio/Inicio ☐ puede unirse a reuniones Skype Empresarial programadas (Skype interfaz de usuario) ☐ puede unirse a reuniones Teams programadas (Teams interfaz de usuario)

COMPROBADO	RESPUESTA
Microsoft Teams Comportamiento del modo 1	☐ Teams en la pantalla Inicio/Inicio ☐ puede unirse a reuniones Skype Empresarial programadas (Skype interfaz de usuario) ☐ puede unirse a reuniones Teams programadas (Teams interfaz de usuario)
Microsoft Teams Comportamiento del modo 2	☐ Teams icono en la pantalla Inicio /Inicio ☐ puede unirse a reuniones Teams programadas ☐ no poder unirse a Skype Empresarial reuniones

Configuración por primera vez para Surface Hub

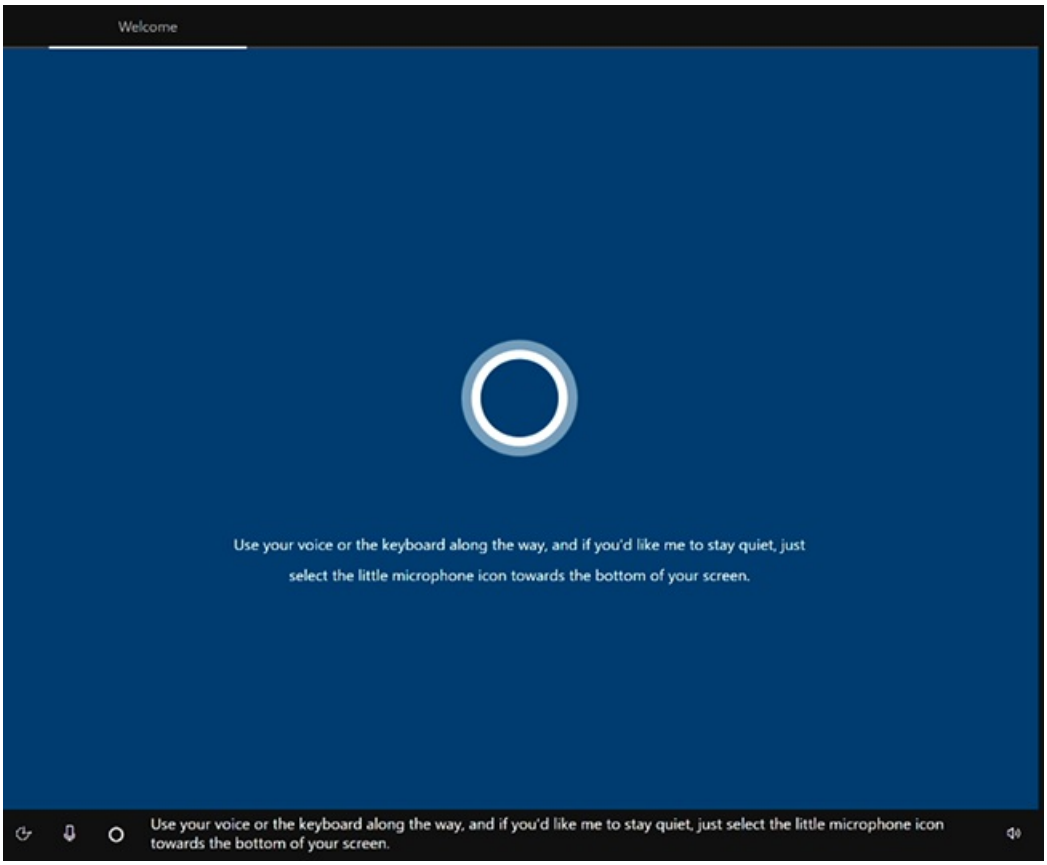
12/01/2022 • 4 minutes to read

La primera vez que Surface Hub, el dispositivo entra automáticamente en el modo de configuración por primera vez para guiarte a través de la configuración de la cuenta y la configuración relacionada.

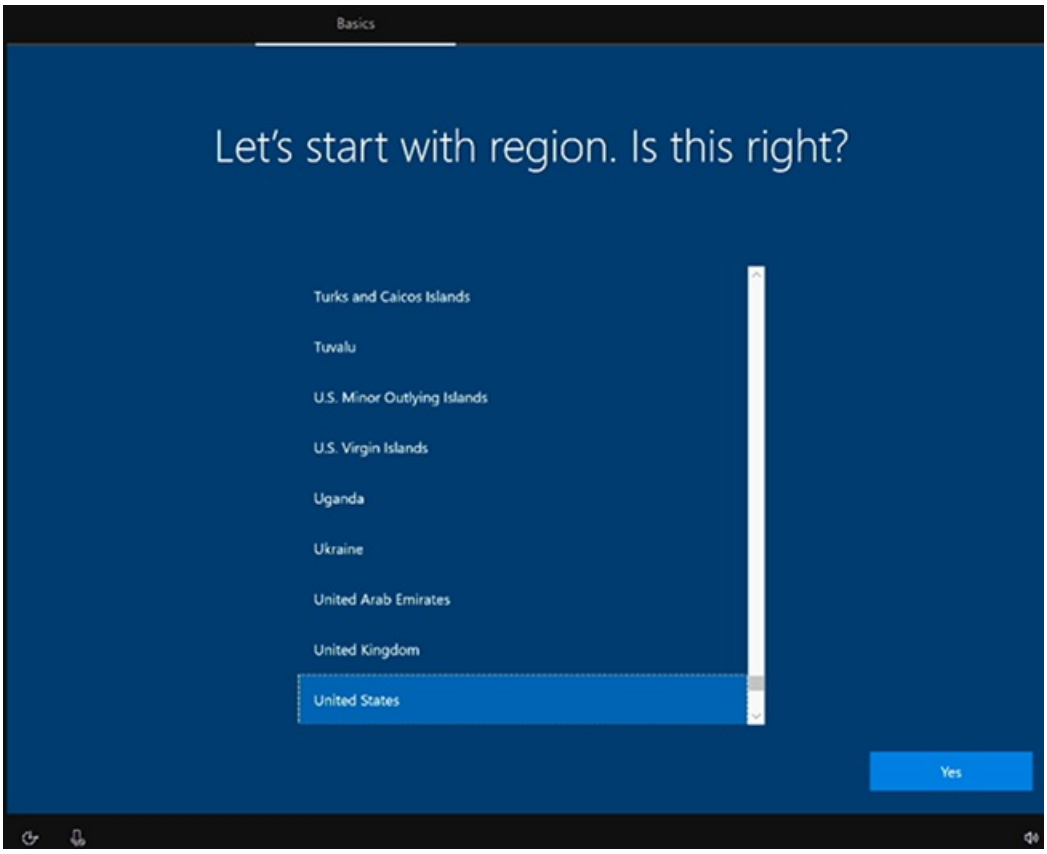
> **TIP**
> Puedes automatizar todo el proceso de configuración con un paquete de aprovisionamiento para garantizar una experiencia coherente en varios Surface Hubs.

Comenzar

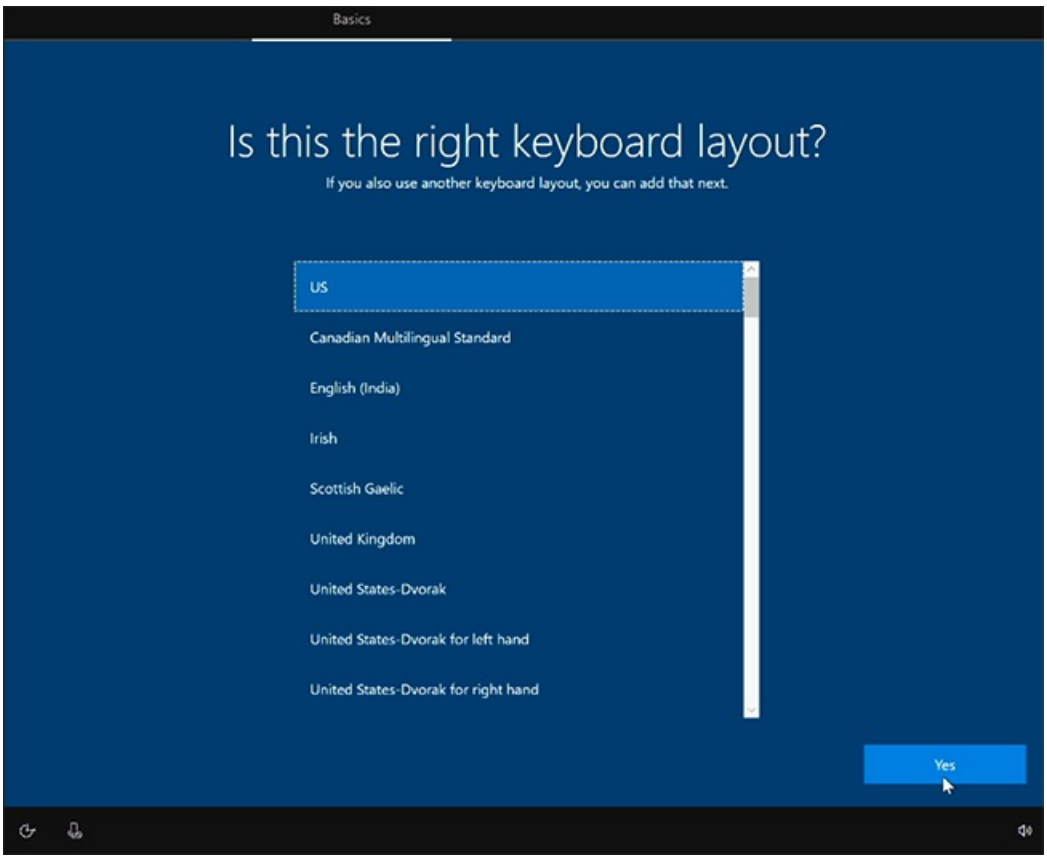
1. De forma predeterminada, Cortana está habilitado para guiarlo a través del proceso. Para desactivar la Cortana, seleccione el icono del micrófono.



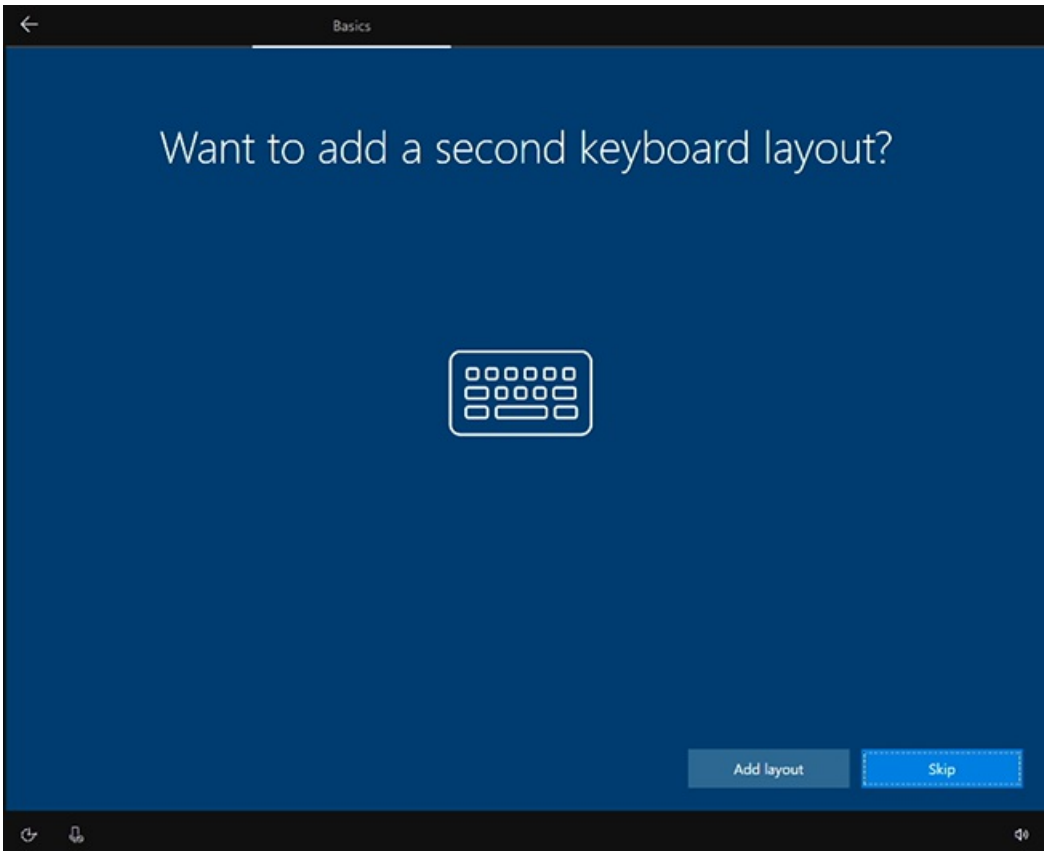
2. **Elige tu región.** Confirme la región detectada automáticamente y seleccione **Sí**.



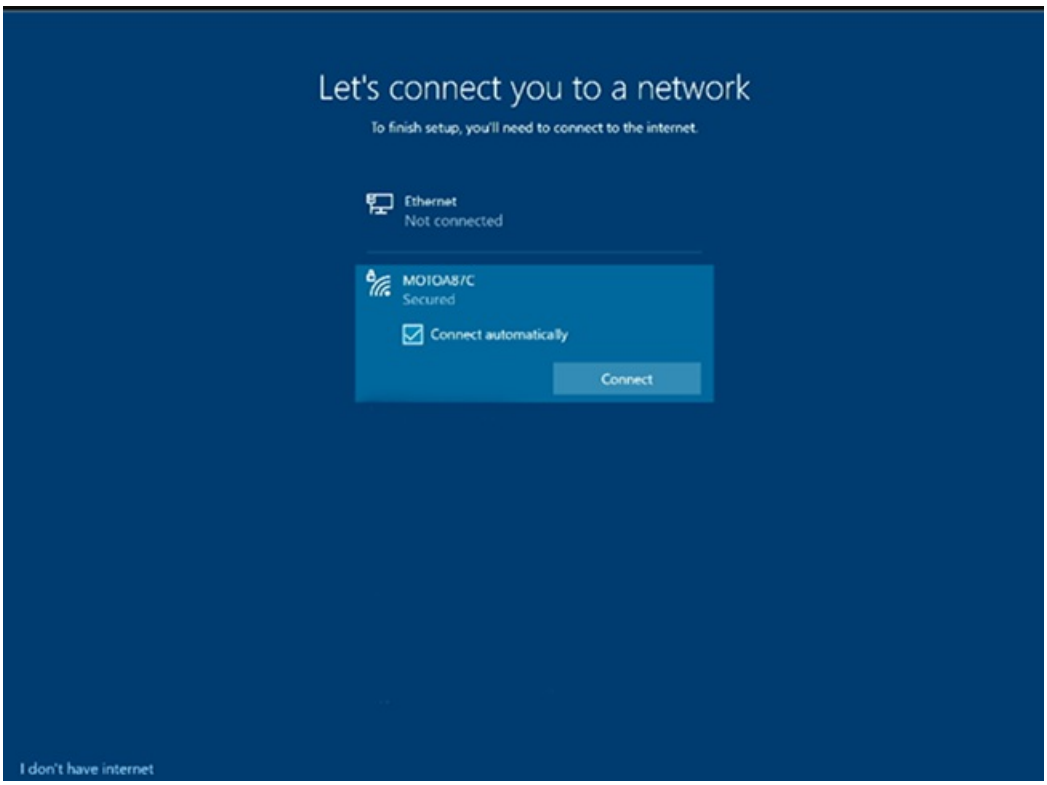
3. **Confirme el diseño del teclado.** Seleccione **Sí**.



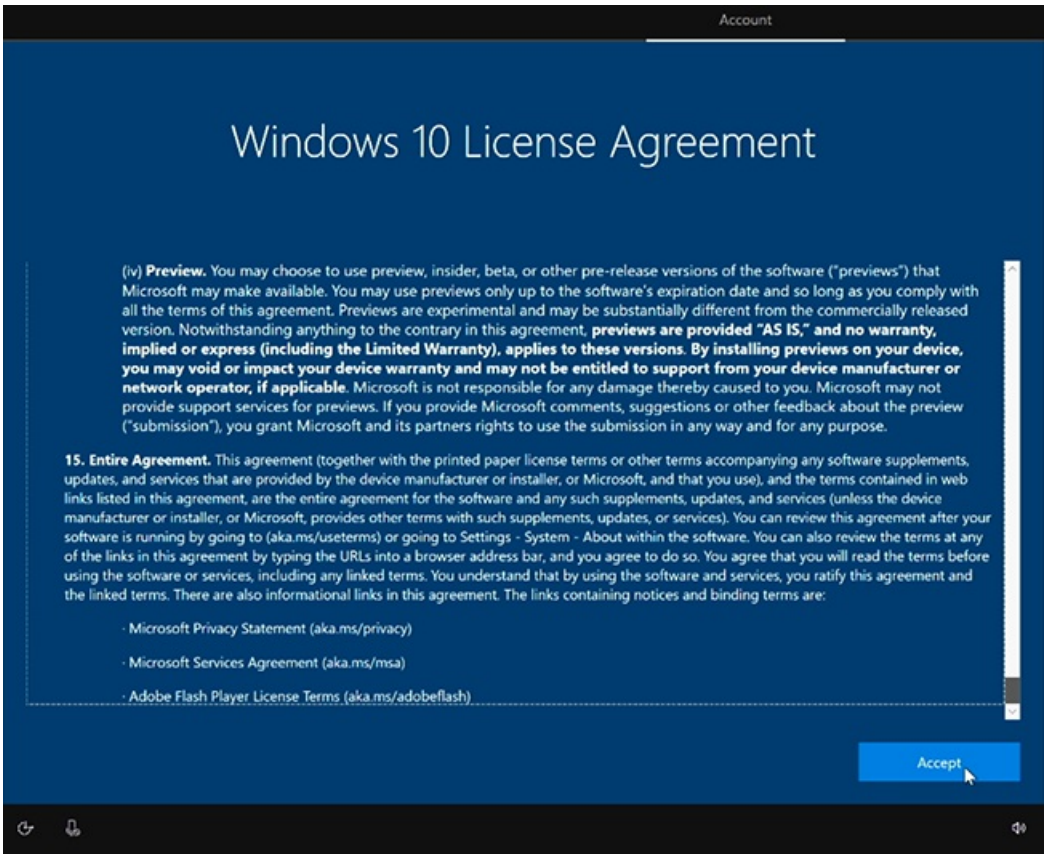
4. Para agregar un segundo teclado, seleccione **Agregar diseño**. De lo contrario, **seleccione Omitir**.



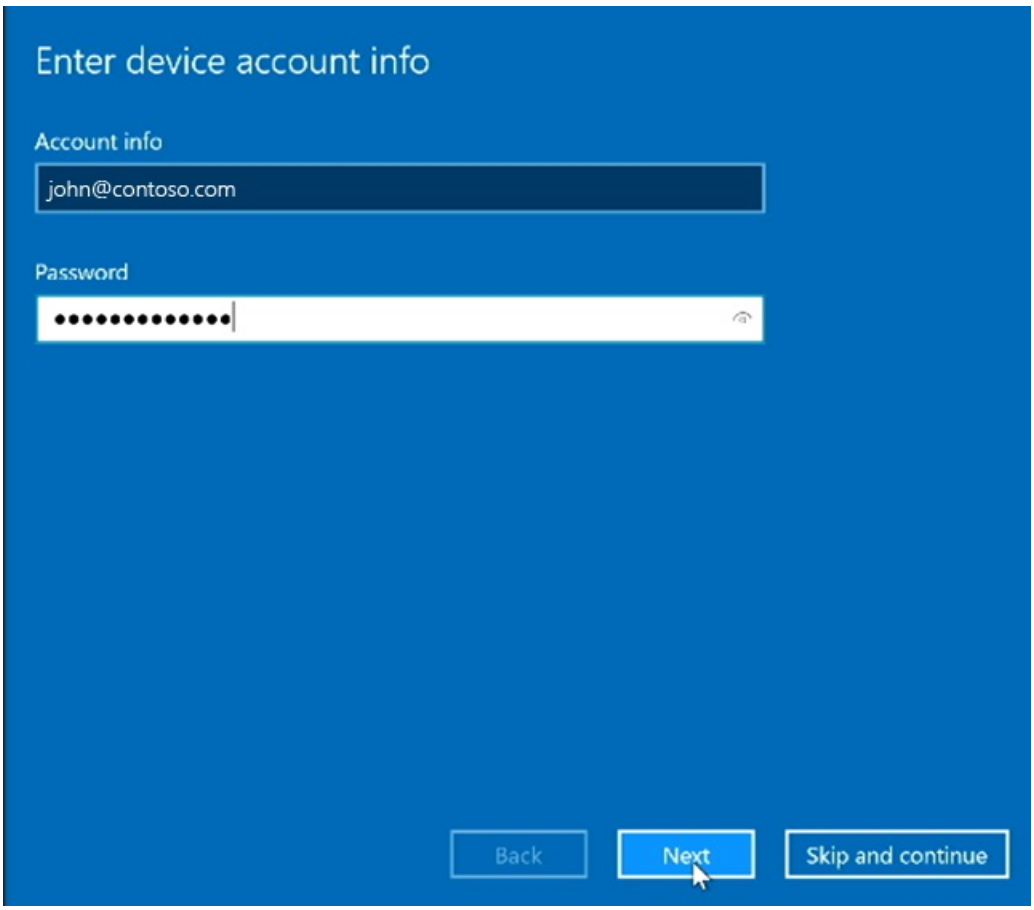
5. **Conectar a una red.** Si ya ha conectado un cable Ethernet, Surface Hub conectará automáticamente a la red. Como alternativa, puede conectarse a una red inalámbrica. **Nota:** No puede conectarse a una red inalámbrica en puntos de acceso (portales cautivos) que redirijan las solicitudes de inicio de sesión al sitio web de un proveedor. Selecciona **Siguiente**.



6. **Acepte Windows 10 de licencia.** Seleccione **Aceptar**.



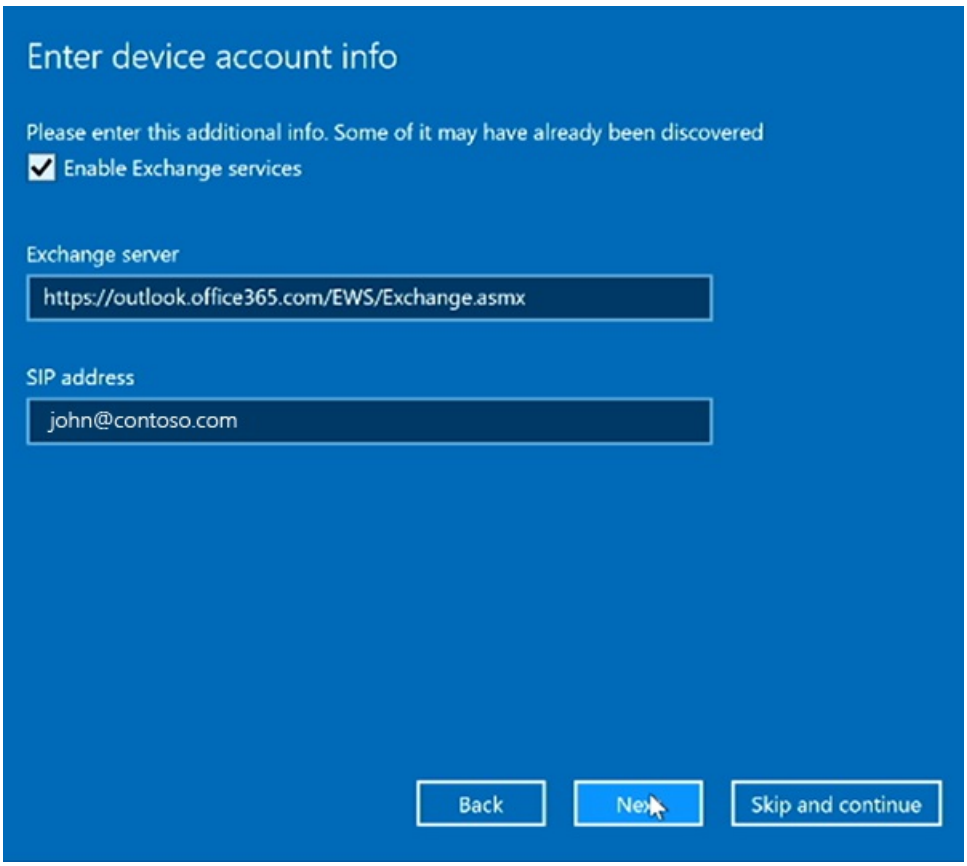
7. **Escribe información de cuenta de** dispositivo con una dirección UPN (user@contoso.com) o una dirección de dominio de nivel inferior (CONTOSO\usuario). Use el formato que coincida con el entorno y escriba la contraseña.



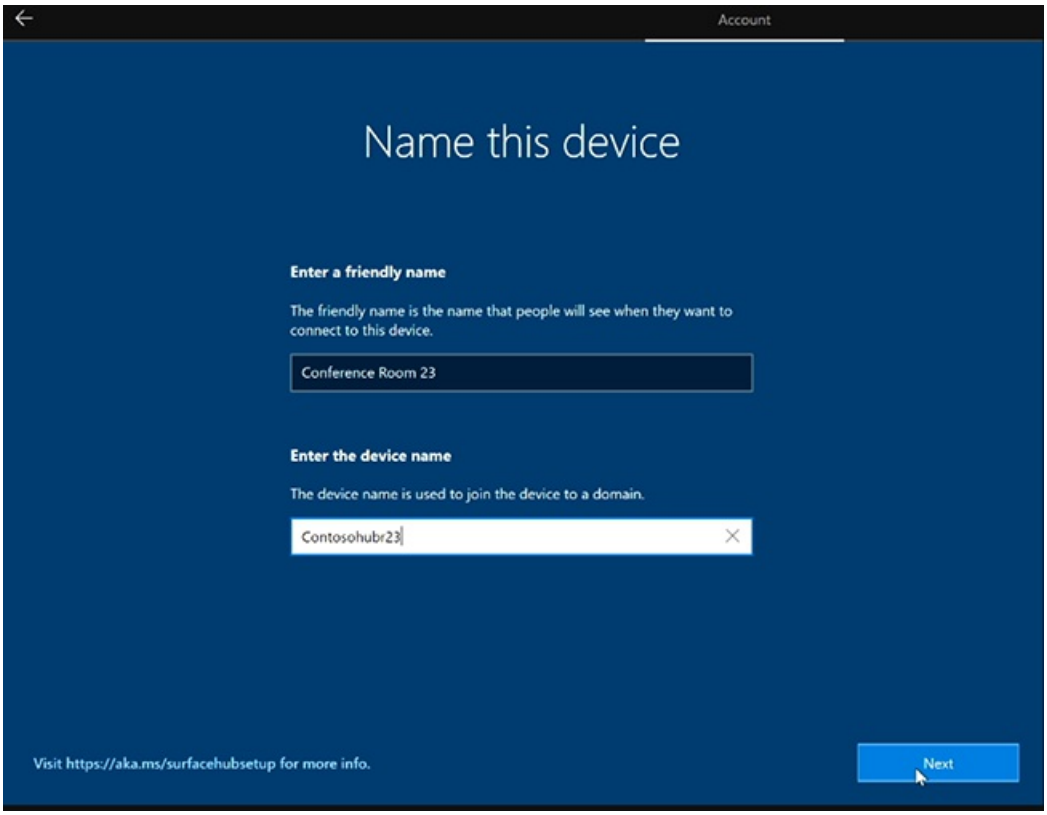
ENTORNO	FORMATO REQUERIDO PARA LA CUENTA DEL DISPOSITIVO
La cuenta de dispositivo se hospeda solo en línea	username@contoso.com
La cuenta de dispositivo solo se hospeda localmente	CONTOSO\user
La cuenta de dispositivo se hospeda en línea y local (híbrida)	CONTOSO\user

> **NOTE**
> Aunque puedes omitir la configuración de una cuenta de dispositivo, el dispositivo no estará totalmente integrado en la infraestructura. Si omites la configuración ahora, puedes agregar una cuenta del dispositivo más adelante mediante la aplicación Configuración.

8. **Escribe la contraseña y** selecciona **Siguiente.**
9. Surface Hub detecta automáticamente la información Exchange servidor y la dirección SIP del dominio especificado en el paso anterior. O, si es necesario, proporcione la dirección Exchange servidor y seleccione **Siguiente**.



10. **Asigne un nombre a este dispositivo.** Escribe un nombre para el dispositivo o usa el sugerido. **Seleccione Siguiente**.



- El **nombre descriptivo** está visible en la esquina inferior izquierda de Surface Hub 2S y se muestra al proyectar al dispositivo.
- El **nombre del dispositivo** identifica el dispositivo cuando está asociado con Active Directory o Azure Active Directory y al inscribir el dispositivo con Intune.

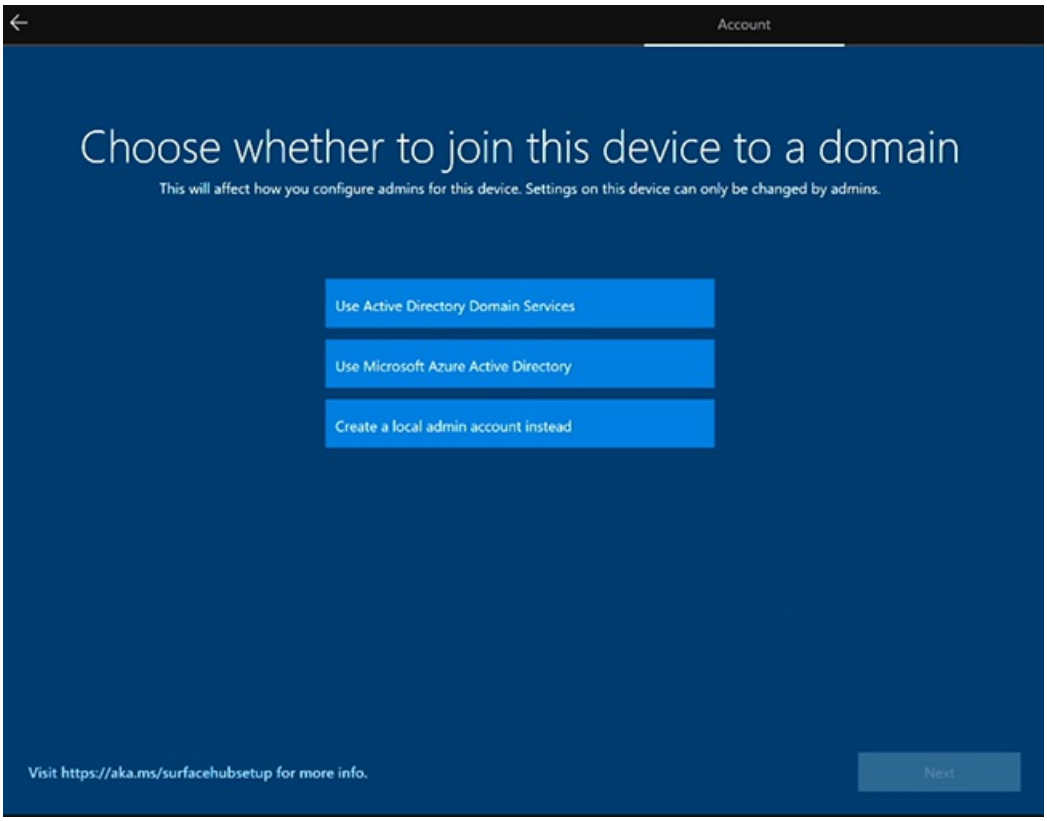
> **NOTE**
> Si quieres habilitar Miracast sobre infraestructura, el nombre del dispositivo debe ser reconocible mediante DNS. Puedes lograrlo permitiendo que Surface Hub se registre automáticamente a través de DNS dinámico, o crear manualmente un registro A o AAAA para el nombre de host del dispositivo Surface Hub.

Configurar cuentas de administrador de dispositivos

Solo puedes configurar administradores de dispositivos durante la configuración por primera vez. Para más información, consulta:

- Surface Hub de dispositivos 2S
- Administración del grupo de administradores

1. **Elija el tipo de cuenta de administrador.** Seleccione una de las siguientes opciones: Servicios de dominio de Active Directory, Azure Active Directory o Administrador local.



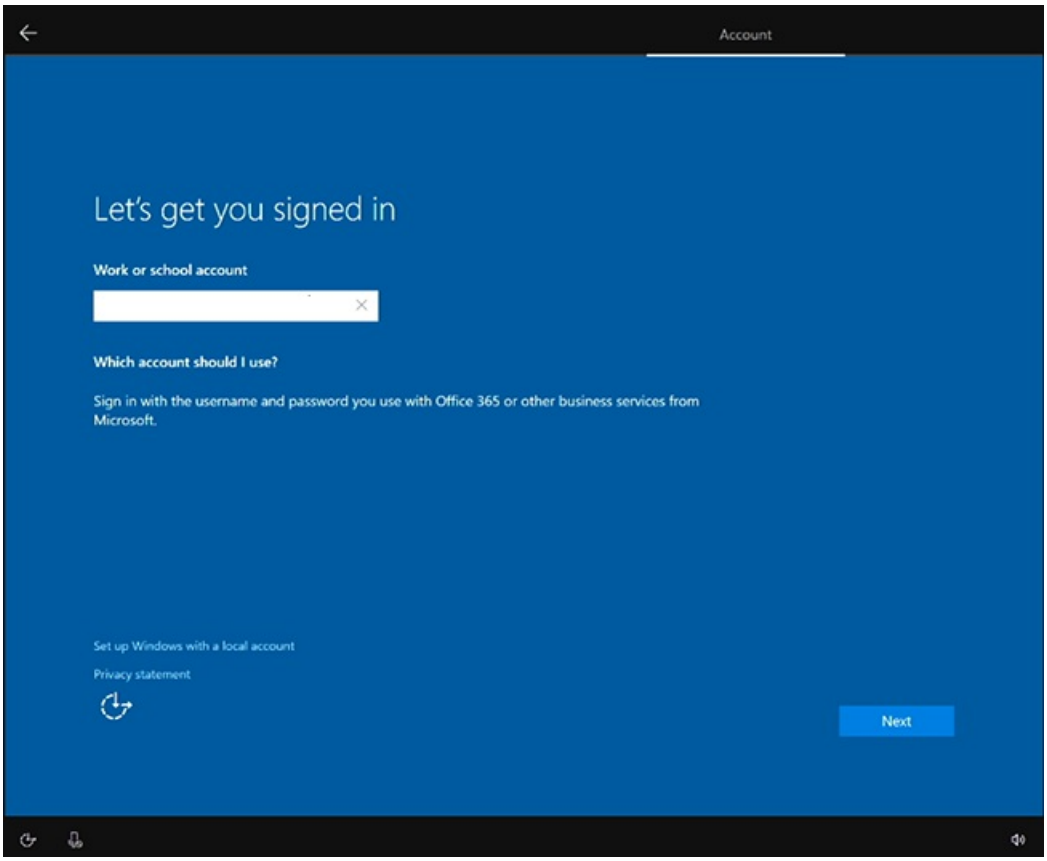
Active Directory Domain Services

1. Si tiene la intención de usar Surface Hub en un entorno local, puede asociar El concentrador con **los servicios de dominio de Active Directory**. Escriba las credenciales de un usuario que tenga permisos para unirse al dispositivo a Active Directory.
2. Selecciona el grupo de seguridad de Active Directory que contiene los miembros que pueden iniciar sesión en la Configuración en Surface Hub 2S.
3. Seleccione **Finalizar**. El dispositivo se reiniciará.

Microsoft Azure Active Directory

1. Si tienes la intención de administrar Surface Hub desde la nube con Microsoft Intune o un proveedor MDM, selecciona **Microsoft Azure Active Directory**.

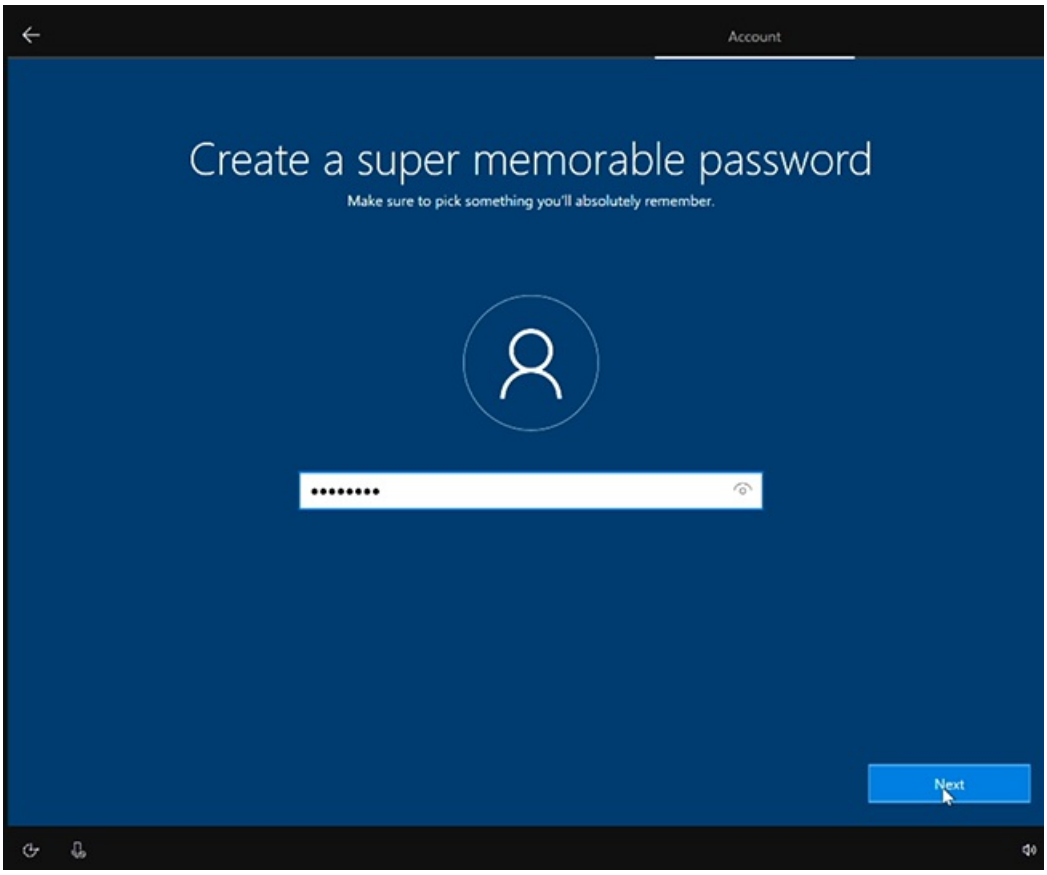
2. Seleccione Siguiente e inicie sesión con una cuenta laboral o educativa. Si se redirige, autentique con la página de inicio de sesión de su organización y proporcione credenciales adicionales si se solicita. De lo contrario, escriba la contraseña y seleccione **Siguiente.**



> **NOTE**
> Para configurar quién puede usar la aplicación Configuración para administrar Surface Hubs, asegúrese de que la inscripción automática de Intune está habilitada en el inquilino antes de unir el dispositivo a Azure AD. Las directivas de Intune se pueden usar para configurar administradores que no son globales en Surface Hubs.

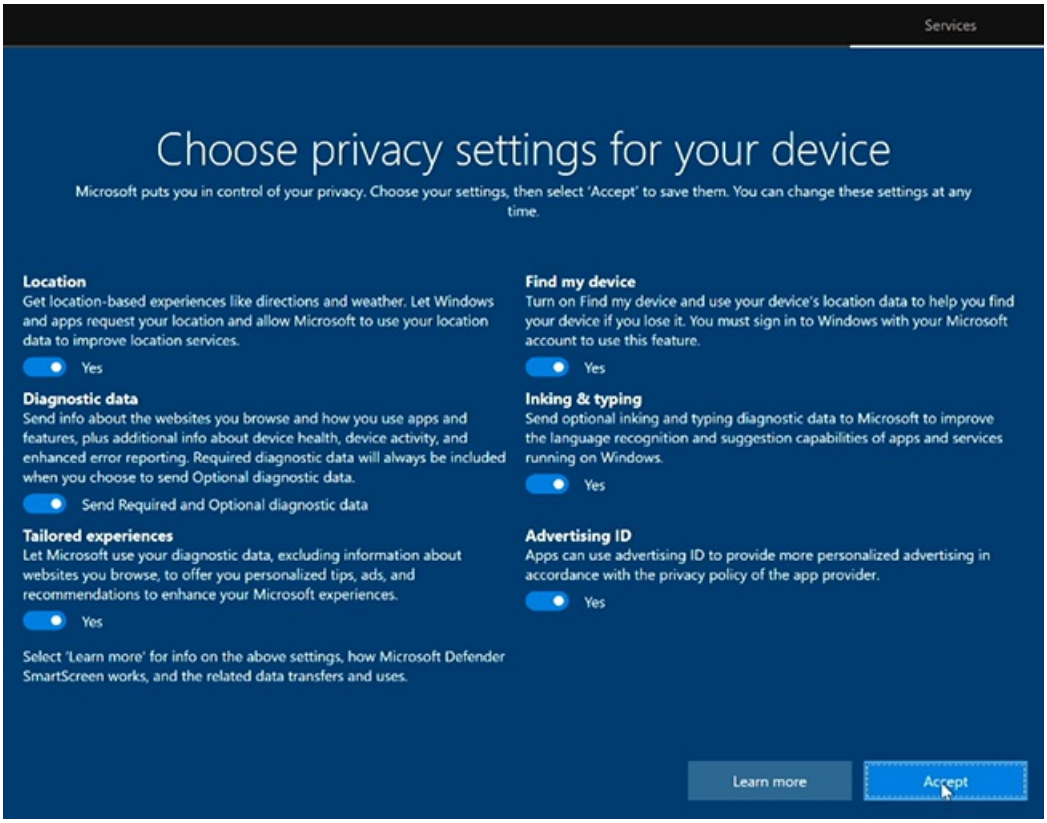
Cuenta de administrador local

- Escriba un nombre de usuario y una contraseña memorable para el administrador local. (Si olvida la contraseña de administrador local, tendrá que recuperar el dispositivo y repetir el proceso de configuración).



Elegir la configuración de privacidad del dispositivo

- Seleccione entre la configuración de privacidad disponible y seleccione **Aceptar.**



Usar paquetes de aprovisionamiento

Puedes personalizar las opciones de configuración por primera vez, lo que te permite garantizar una experiencia coherente en varios Surface Hubs.

1. Para empezar, revise la documentación de Crear paquetes de aprovisionamiento y guarde el paquete de aprovisionamiento en una unidad usb.

2. Inserte la unidad usb en uno de los puertos USB antes de iniciar el proceso de configuración.
3. Cuando se le pida, elija el paquete de aprovisionamiento que desea usar.
4. Si creaste un archivo CSV de varios dispositivos, podrás elegir una configuración de dispositivo.
5. Siga las instrucciones para completar el programa de instalación por primera vez.

Administrar Microsoft Surface Hub

12/01/2022 • 2 minutes to read

Después de la configuración inicial de Microsoft Surface Hub, la configuración y la configuración del dispositivo se pueden modificar o cambiar de un par de maneras:

- **Administración local** - Cada Surface Hub se puede configurar localmente con la aplicación **Configuración** en el dispositivo. Para impedir que usuarios no autorizados cambien la configuración, la aplicación Configuración requiere credenciales de administrador para abrir la aplicación. Para obtener más información, consulta Administración local para la configuración de Surface Hub.
- **Administración remota:** Surface Hub a los administradores de TI administrar la configuración y las directivas con un proveedor de administración de dispositivos móviles (MDM), como Microsoft Intune, Microsoft Endpoint Configuration Manager y otros proveedores de terceros. Además, los administradores pueden supervisar Surface Hubs con Azure Monitor. Para obtener más información, consulta Administrar la configuración conun proveedor MDM y Supervisar Surface Hubs con Azure Monitor para realizar un seguimiento de su estado.

> **NOTE**
> Estos métodos de administración no son mutuamente excluyentes. Los dispositivos pueden administrarse tanto local como remotamente, si así lo eliges. Sin embargo, las directivas y la configuración de MDM sobrescribirán los cambios locales cuando el Surface Hub se sincronice con el servidor de administración.

En esta sección

Obtén información sobre cómo administrar y actualizar Surface Hub.

TEMA	DESCRIPCIÓN
Administración remota de Surface Hub	Temas relacionados con la administración remota del Surface Hub. Incluye instalar aplicaciones, administrar la configuración con MDM y supervisar con Operations Management Suite.
Administrar la configuración de Surface Hub	Temas relacionados con la administración de la configuración de Surface Hub: accesibilidad, cuenta del dispositivo, restablecimiento del dispositivo, nombre de dominio completo, configuración de Windows Update y red inalámbrica
Instalar aplicaciones en Surface Hub	Los administradores pueden instalar aplicaciones desde Microsoft Store o la Microsoft Store para Empresas.
Configurar el menú Inicio de Surface Hub	Usar MDM para personalizar el menú Inicio para Surface Hub.
Configurar y usar Microsoft Whiteboard	La actualización más reciente de Microsoft Whiteboard incluye la capacidad para que dos dispositivos Surface Hub colaboren en tiempo real en la misma pizarra.

TEMA	DESCRIPCIÓN
Finalizar una reunión con Terminar la sesión	Al final de una reunión, los usuarios pueden presionar **Terminar la sesión** para limpiar los datos confidenciales y preparar el dispositivo para la próxima reunión.
Iniciar sesión en Surface Hub con Microsoft Authenticator	Puedes iniciar sesión en un dispositivo Surface Hub sin una contraseña con la aplicación Microsoft Authenticator, disponible en Android e iOS.
Guardar la clave de BitLocker	Todos los Surface Hubs se configuran automáticamente con el software de cifrado de unidad de BitLocker. Microsoft recomienda encarecidamente que te asegures de hacer una copia de seguridad de las claves de recuperación de BitLocker.
Conectarse a otros dispositivos y mostrar su contenido con Surface Hub	Puedes conectar otro dispositivo a tu Surface Hub para mostrar su contenido.
Miracast en la red inalámbrica o LAN existente	Puedes usar Miracast en tu red inalámbrica o LAN para conectarte a Surface Hub.
Habilitar la autenticación por cable 802.1X	Se han habilitado políticas MDM de autenticación por cable 802.1x en dispositivos de Surface Hub.
Uso de un sistema de control de sala	Los sistemas de control de la sala se pueden usar con tu Microsoft Surface Hub.
Uso de la herramienta de recuperación de Surface Hub	Usa la Surface Hub recuperación de archivos para volver a crear una imagen del SSD Surface Hub.
Reemplazo de SSD de Surface Hub	Obtenga información sobre cómo quitar y reemplazar la unidad de estado sólido en su Surface Hub.

Temas relacionados

- Ver modo de presentación de Power BI en Surface Hub y Windows 10

Administrar Microsoft Edge en Surface Hub

12/01/2022 • 3 minutes to read

Use Microsoft Edge de explorador para configurar la configuración del explorador Microsoft Edge a través de cualquiera de los siguientes métodos:

- Microsoft Intune
- El proveedor de administración de dispositivos móviles (MDM) preferido que admite la ingesta de ADMX
- Aprovisionar paquetes con admx ingestion en Windows Configuration Designer

> **TIP**
> El gesto de deslizar el dedo hacia abajo desde la parte superior de la pantalla para salir del modo de pantalla completa requiere dos dedos con el nuevo Microsoft Edge. La acción salir de pantalla completa también está disponible en el menú contextual que se muestra después de presionar durante mucho tiempo.

Directivas Microsoft Edge predeterminadas para Surface Hub

Microsoft Edge está preconfigurado con los siguientes conjuntos de directivas para proporcionar una experiencia optimizada para Surface Hub.

> **TIP**
> Se recomienda conservar el valor predeterminado para esta configuración de directiva.

CONFIGURACIÓN DE DIRECTIVA	EXPERIENCIA RECOMENDADA	VALOR PREDETERMINADO
AutoImportAtFirstRun	No importe automáticamente los tipos de datos y la configuración de Microsoft Edge (versión anterior). Esto evita cambiar los perfiles de los usuarios que han iniciado sesión con la configuración compartida de la Surface Hub.	4
BackgroundModeEnabled	Permitir Microsoft Edge los procesos para seguir ejecutándose en segundo plano incluso después de que se cierre la última ventana del explorador, lo que permite un acceso más rápido a las aplicaciones web durante una sesión.	1
BrowserAddProfileEnabled	No permitir que los usuarios creen nuevos perfiles en Microsoft Edge. Esto simplifica la experiencia de exploración y de sesión.	0

CONFIGURACIÓN DE DIRECTIVA	EXPERIENCIA RECOMENDADA	VALOR PREDETERMINADO
BrowserGuestModeEnabled	Permite que solo un usuario inicie sesión en Microsoft Edge. Esto simplifica la experiencia de exploración y de sesión	0
BrowserSignin	Permite a los usuarios disfrutar de single Sign-On (SSO) en Microsoft Edge. Cuando un usuario ha iniciado sesión Surface Hub, sus credenciales pueden fluir a los sitios web compatibles sin necesidad de que se vuelvan a autenticar.	1
ExtensionInstallBlockList	Impide que los usuarios que no son administradores instalen nuevas extensiones en Microsoft Edge. Para configurar una lista de extensiones que se instalarán de forma predeterminada, use ExtensionInstallForcelist.	*
HideFirstRunExperience	Oculta la primera experiencia de ejecución y la pantalla de presentación que normalmente se muestra cuando los usuarios ejecutan Microsoft Edge por primera vez. Dado Surface Hub es un dispositivo compartido, esto simplifica la experiencia del usuario.	1
InPrivateModeAvailability	Deshabilita el modo InPrivate. Dado que End Session ya borra los datos de exploración, esto simplifica la experiencia de exploración y de inicio de sesión.	1
NewTabPageSetFeedType	Muestra la Office 365 de fuentes en páginas de pestañas nuevas. Cuando un usuario ha iniciado sesión Surface Hub, esto permite un acceso rápido a sus archivos y contenido en Office 365.	1
NonRemovableProfileEnabled	Cuando un usuario ha iniciado sesión Surface Hub, se creará un perfil no extraíble con su cuenta organizativa. Esto simplifica la experiencia de single Sign-On (SSO).	1
PrintingEnabled	Deshabilita la impresión en Microsoft Edge. Surface Hub no admite la impresión.	0
ProActiveAuthEnabled	Permite Microsoft Edge autenticación proactiva de usuarios que han iniciado sesión con servicios Microsoft. Esto simplifica la experiencia de single Sign-On (SSO).	1

CONFIGURACIÓN DE DIRECTIVA	EXPERIENCIA RECOMENDADA	VALOR PREDETERMINADO
PromptForDownloadLocation	Guarda automáticamente los archivos en la carpeta Descargas, en lugar de preguntar a los usuarios dónde guardar el archivo. Esto simplifica la experiencia de exploración.	0

> **IMPORTANT**
> Actualmente, las aplicaciones web progresivas (PWA) no se admiten en el Windows 10 Team operativo. Tenga en cuenta también que Microsoft Edge configuración de directiva webAppInstallForceList no se admite en Surface Hub.

Configurar Microsoft Edge actualizaciones

De forma predeterminada, Microsoft Edge se actualiza automáticamente. Use Microsoft Edge de actualización para configurar la configuración de Microsoft Edge Update. Tenga en cuenta que Surface Hub no admite la configuración de directiva **CreateDesktopShortcut,** ya que Surface Hub no usa métodos abreviados de escritorio.

> **TIP**
> Microsoft Edge requiere conectividad a Internet para posibilitar sus funciones. Agregue las direcciones URL de dominio necesarias a la lista Permitir para garantizar las comunicaciones a través de firewalls y otros mecanismos de seguridad.

Vínculos relacionados

- Documentación de Microsoft Edge

PowerShell para Surface Hub (v1)

12/01/2022 • 32 minutes to read

> **NOTE**
> Esta página incluye scripts de PowerShell destinados al Surface Hub original (v1). Para ver los scripts de creación de cuentas más recientes para Surface Hub 2S, consulta Crear y probar una cuenta de dispositivo.

> **NOTE**
> Vea también Autenticación moderna y scripts desatendidos en Exchange Online PowerShell V2

Requisitos previos

Para ejecutar correctamente estos scripts de PowerShell, necesitarás instalar los siguientes requisitos previos:

- Microsoft Online Services - Ayudante para el inicio de sesión para RTW de profesionales de TI
- Módulo Microsoft Azure Active Directory para Windows PowerShell (versión de 64 bits)
- Módulo Windows PowerShell para Skype Empresarial Online

Scripts de PowerShell para administradores de Surface Hub

¿Qué hacen los scripts?

- Crear cuentas de dispositivo para configuraciones solo mediante bosque único local (Microsoft Exchange y Skype 2013 y versiones posteriores solamente) o en línea (Microsoft Office 365), que están configurados correctamente para Surface Hub.
- Validar cuentas de dispositivo existentes para cualquier configuración (local o en línea) para garantizar que son compatibles con Surface Hub.
- Proporcionar una plantilla base para cualquier persona que desee crear sus propios scripts de creación o de validación de cuentas de dispositivo.

¿Qué necesita para ejecutar los scripts?

- Acceso de PowerShell remoto al dominio o inquilino de su organización, servidores de Exchange y Skype Empresarial.
- Credenciales de administrador para el dominio o inquilino de su organización, servidores de Exchange y

Skype Empresarial.

> **NOTE**
> Si vas a crear una nueva cuenta o a modificar una ya existente, el script de validación comprobará que la cuenta del dispositivo está correctamente configurada. Siempre se debe ejecutar el script de validación antes de agregar una cuenta del dispositivo a Surface Hub.

Ejecutando los scripts

Los scripts de creación de cuenta podrán:

- Solicite credenciales de administrador.
- Crea cuentas de dispositivo en tu dominio/inquilino.
- Crea o asigna una directiva de ActiveSync compatible con Surface Hub a las cuentas del dispositivo.
- Establecer varios atributos de las cuentas creadas en Exchange y Skype Empresarial.
- Asignar licencias y permisos a las cuentas creadas.

Estos son los atributos que establecen los scripts:

CMDLET	ATRIBUTO	VALOR
Set-Mailbox	RoomMailboxPassword	User-provided
	EnableRoomMailboxAccount	True
	Tipo	Sala
Set-CalendarProcessing	AutomateProcessing	AutoAccept
	RemovePrivateProperty	False
	DeleteSubject	False
	DeleteComments	False
	AddOrganizerToSubject	False
	AddAdditionalResponse	True
	AdditionalResponse	"Esta es una sala de Surface Hub."
New-MobileDeviceMailboxPolicy	PasswordEnabled	False
	AllowNonProvisionableDevices	True

CMDLET	ATRIBUTO	VALOR
Enable-CSMeetingRoom	RegistrarPool	User-provided
	SipAddress	Establecer en el nombre principal de usuario (UPN) de la cuenta del dispositivo
Set-MsolUserLicense (solo O365)	AddLicenses	User-provided
Set-MsolUser (solo O365)	PasswordNeverExpires	True
Set-AdUser (solo local)	Habilitado	True
Set-AdUser (solo local)	PasswordNeverExpires	True

Scripts de creación de cuenta

Estos scripts crearán una cuenta del dispositivo para ti. Puedes usar el Script de comprobación de cuenta para asegurarte de que se ejecutan correctamente.

Los scripts de creación de cuenta no pueden modificar una cuenta ya existente, pero se pueden usar para ayudarte a comprender qué cmdlets deben ejecutarse para configurar correctamente la cuenta existente.

Crear una cuenta local

```
# 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
```

```
    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"
}
```

Crear una cuenta del dispositivo mediante Office 365

Crea una cuenta como se describe en Crear una cuenta de dispositivo con Office 365.

```
# 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"
}
```

Script de verificación de cuenta

Este script valida la cuenta de dispositivo creada anteriormente en Surface Hub y Surface Hub 2S, independientemente del método que se haya usado para crearla. Este script es básicamente correcto o incorrecto. Si se produce un error en una de las pruebas, se mostrará un mensaje de error detallado, pero si se superan todas las pruebas, el resultado final será un informe de resumen. Por ejemplo, puedes ver:

```
15 tests executed
0 failures
2 warnings
15 passed
```

No se mostrarán los detalles de la configuración específica.

```
# 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
```

```
($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
```

Habilitar Skype Empresarial

Este script habilitará Skype Empresarial en una cuenta del dispositivo. Úsalo solo si Skype Empresarial no se había habilitado anteriormente durante la creación de la cuenta.

```
## 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()
```

```
$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
```

Cmdlets útiles

Creación de una directiva de ActiveSync compatible con Surface Hub

Para que Surface Hub use los servicios de Exchange, se debe aprovisionar una cuenta del dispositivo configurada con una directiva de ActiveSync compatible en el dispositivo. Esta directiva tiene los siguientes requisitos:

```
PasswordEnabled == 0
```

En los siguientes cmdlets, `$strPolicy` está el nombre de la directiva de ActiveSync y `$strRoomUpn` es el UPN de la cuenta del dispositivo al que quieres aplicar la directiva.

Tenga en cuenta que para poder ejecutar los cmdlets, debe establecer una sesión remota de PowerShell y:

- Tu cuenta de administrador debe tener PowerShell remoto habilitado. Esto permite al administrador usar los cmdlets de PowerShell que necesita el script. (Este permiso se puede establecer mediante `set-user $admin -RemotePowerShellEnabled $true`)
- Tu cuenta de administrador debe tener el rol "Restablecer contraseña" si tienes previsto ejecutar los scripts de creación. Esto permite que el administrador cambie la contraseña de la cuenta, algo necesario para el script. El rol Restablecer contraseña se puede habilitar mediante el Centro de admin. de Exchange.

Crear la directiva.

```
# Create new policy with PasswordEnabled == false
New-MobileDeviceMailboxPolicy -Name $strPolicy -PasswordEnabled $false –AllowNonProvisionableDevices $true
```

Para aplicar la directiva, el buzón no puede ser del tipo sala, por lo que se tiene que convertir en un usuario primero.

```
# Convert user to regular type
Set-Mailbox $strRoomUpn -Type Regular
# Set policy for account
Set-CASMailbox $strRoomUpn -ActiveSyncMailboxPolicy $strPolicy
```

Ahora la cuenta del dispositivo solo se debe convertir de nuevo en un tipo sala.

```
# Convert back to room mailbox
Set-Mailbox $strRoomUpn -Type Room
```

Permitir id. de dispositivo para ActiveSync

Para permitir una cuenta `$strRoomUpn`, ejecuta el siguiente comando:

```
Set-CASMailbox –Identity $strRoomUpn –ActiveSyncAllowedDeviceIDs “<ID>”
```

Para buscar el id. del dispositivo, ejecuta:

```
Get-ActiveSyncDevice -Mailbox $strRoomUpn
```

De este modo se recupera la información del dispositivo para cada dispositivo en el que se haya aprovisionado la cuenta, incluida la propiedad `DeviceId`.

Aceptar o rechazar automáticamente convocatorias de reunión

Para que una cuenta del dispositivo acepte o rechace automáticamente convocatorias de reunión en función de su disponibilidad, el atributo **AutomateProcessing** se debe establecer en **AutoAccept**. Se recomienda esta acción para evitar el solapamiento de reuniones.

```
Set-CalendarProcessing $strRoomUpn -AutomateProcessing AutoAccept
```

Aceptar convocatorias de reunión externas

Para que una cuenta del dispositivo acepte convocatorias de reunión externas (una convocatoria de reunión desde una cuenta que no esté en el mismo dominio o inquilino), la cuenta del dispositivo se debe establecer para permitir el procesamiento de convocatorias de reunión externas. Una vez establecida, la cuenta del dispositivo aceptará o rechazará automáticamente las convocatorias de reunión desde cuentas externas, así como desde cuentas locales.

> **NOTE**
> Si el **atributo AutomateProcessing** no está establecido en **AutoAccept**, esta configuración no tendrá ningún efecto.

```
Set-CalendarProcessing $strRoomUpn -ProcessExternalMeetingMessages $true
```

Administración remota de Surface Hub

12/01/2022 • 2 minutes to read

En esta sección

TEMA	DESCRIPCIÓN
Administrar la configuración con un proveedor de MDM	Surface Hub proporciona una solución de administración empresarial para ayudar a los administradores de TI a administrar directivas y aplicaciones empresariales en estos dispositivos con una solución de administración de dispositivos móviles (MDM).
Supervisar Surface Hub	La supervisión de Surface Hub dispositivos está habilitada a través de Azure Monitor.
Actualizaciones de Windows	Puede administrar actualizaciones Windows en su Surface Hub estableciendo la ventana de mantenimiento, aplazando actualizaciones o usando Windows Update for Business (WUfB).

Administrar Surface Hub con un proveedor MDM

12/01/2022 • 7 minutes to read

Surface Hub permite a los administradores de TI administrar la configuración y las directivas mediante un proveedor de administración de dispositivos móviles (MDM), como Microsoft Intune. Surface Hub tiene un componente de administración integrado para comunicarse con el servidor de administración. No es necesario instalar clientes adicionales en el dispositivo.

Inscripción de Surface Hub en la administración de MDM

Puedes inscribir Surface en Microsoft Intune otro proveedor mdm a través de la inscripción manual o automática.

Inscripción manual

1. Abre la **Configuración** e inicia sesión como administrador local. Seleccione **Surface Hub** > **Administración de dispositivos** y, a continuación, seleccione **+Administración de dispositivos**.
2. Se te pedirá que inicies sesión con la cuenta que usarás para tu proveedor mdm. Después de autenticar, el dispositivo se inscribe automáticamente con el proveedor mdm.

> **TIP**
> Si usa Intune y no se detecta la dirección del servidor, escriba **manage.microsoft.com**.

> **NOTE**
> La inscripción de MDM usa los detalles de la cuenta proporcionados para la autenticación. La cuenta debe tener permisos para inscribir un dispositivo Windows, así como una licencia de Intune (o las licencias de inscripción equivalentes configuradas en el proveedor MDM de terceros).

Inscripción automática: afiliada a Azure AD

Durante el proceso de configuración inicial, al asociar Surface Hub con un inquilino de Azure Active Directory (AD) que tenga habilitada la inscripción automática de Intune, el dispositivo se inscribirá automáticamente en Intune. Para obtener más información, consulte Intune enrollment methods for Windows devices. La afiliación de Azure AD y la inscripción automática de Intune son necesarias para que Surface Hub sea un "dispositivo compatible" en Intune.

Administrar Surface Hub Windows 10 Team configuración con Intune

El bloque de creación fundamental de la administración de la configuración de directivas en Intune y otros proveedores de MDM es el protocolo open mobile Alliance-Device management (OMA-DM) basado en XML. Windows 10 implementa OMA-DM XML a través de uno de los muchos proveedores de servicios de configuración (CSP) disponibles con nombres como AccountManagement CSP, DeviceStatus CSP, WiFi-CSP, entre otros. Para obtener una lista completa, consulte LOSP compatibles con Microsoft Surface Hub.

Microsoft Intune y otros proveedores de MDM usan CSP para ofrecer una interfaz de usuario que te permita configurar las opciones de directiva en los perfiles de configuración. Intune usa el CSP de Surface Hub para su perfil integrado (restricciones de **dispositivos (Windows 10 Team),** lo que te permite configurar opciones básicas como impedir que Surface Hub "se desenlome" cada vez que alguien se mueva cerca dentro de su intervalo de proximidad. Para administrar la configuración del concentrador y las características fuera del perfil

integrado de Intune, deberá usar un perfil personalizado, como se muestra a continuación.

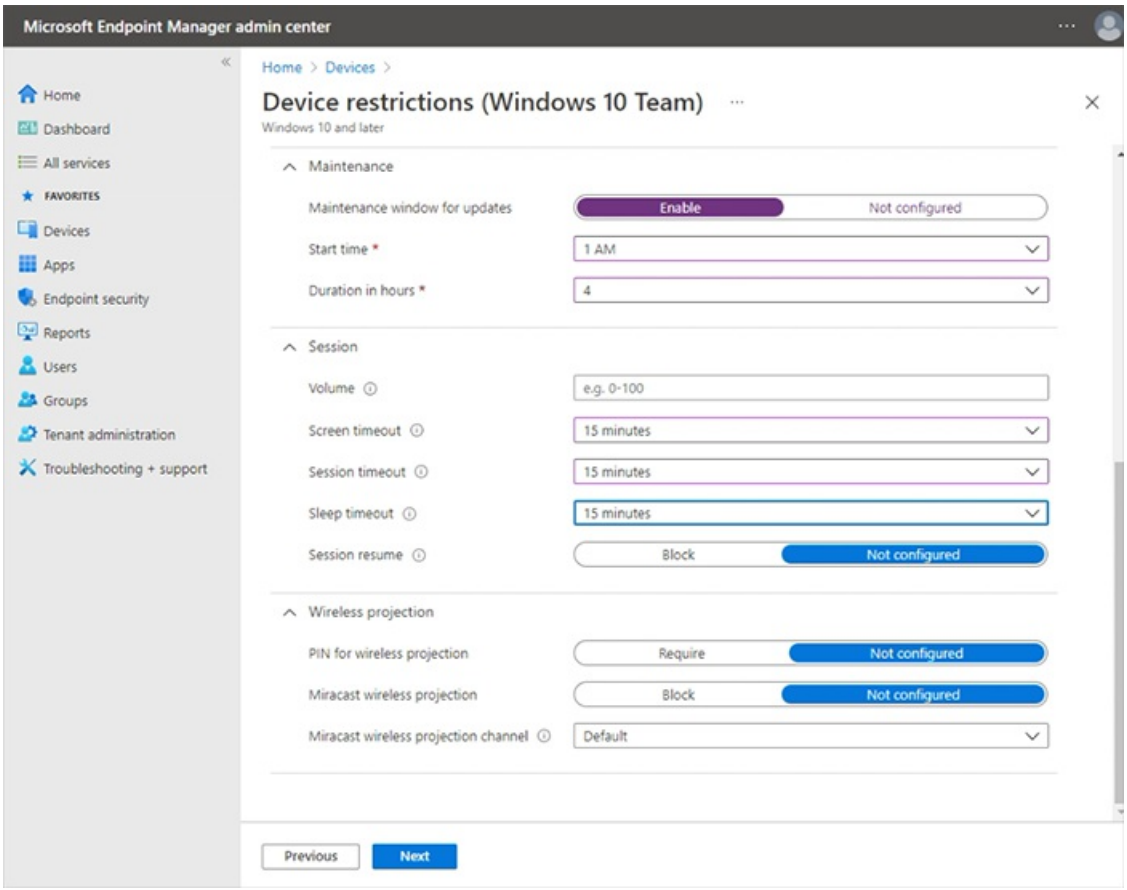
En resumen, las opciones para configurar y administrar la configuración de directivas en Intune incluyen lo siguiente:

- **Crear un perfil de restricción de dispositivo.** Usa el perfil integrado de Intune y configura la configuración directamente en la interfaz de usuario de Intune. Consulta Crear perfil de restricción de dispositivos.
- **Crear un perfil de configuración de dispositivo.** Seleccione una plantilla centrada en una característica o tecnología específica, como Microsoft Defender o certificados de seguridad. Consulta Crear perfil de configuración de dispositivo.
- **Crear un perfil de configuración personalizado.** Amplíe el ámbito de administración mediante un identificador uniforme de recursos (URI de OMA) de OMA desde cualquiera de los CSP admitidos en Microsoft Surface Hub. Consulte Crear perfil de configuración personalizado.

> **NOTE**
> Los perfiles deben asignarse a grupos de dispositivos que contengan los dispositivos Surface Hub inscritos.

Crear perfil de restricción de dispositivos

1. Inicie sesión en el **Microsoft Endpoint Manager de administración**, seleccione **** > **Perfiles de configuración de dispositivos** > **+ Crear perfil**.
2. En **Plataforma**, **seleccione Windows 10 y versiones posteriores** >
3. En ****Tipo de**perfil,** seleccione **Plantillas** y, a continuación, **seleccione Restricciones de dispositivo (Windows 10 Team)**
4. Seleccione **Crear**, agregar un nombre y, a continuación, **seleccione Siguiente.**
5. Ahora puede examinar y elegir entre la configuración de restricción de dispositivos preestablecida para Surface Hub en las siguientes categorías: Aplicaciones y experiencia, Información operativa de Azure, Mantenimiento, Sesión y proyección inalámbrica. En el ejemplo que se muestra en la figura siguiente se especifica una ventana de mantenimiento de 4 horas y un tiempo de espera de 15 minutos para la pantalla, el suspensión y la reanudación de la sesión.



Para obtener más información acerca de la creación y administración de perfiles, vea Restringir las características de dispositivosmediante la directiva en Microsoft Intune .

Para obtener más información acerca de cómo administrar las Surface Hub y la configuración, consulta Surface Hub Windows 10 Team restricciones de dispositivos en Microsoft Intune

Crear perfil de configuración de dispositivo

1. Inicie sesión en el **Microsoft Endpoint Manager de administración,**seleccione **Perfiles** > **de configuración de dispositivos** > **+ Crear perfil**.
2. En **Plataforma**, **seleccione Windows 10 y versiones posteriores** >
3. En **Tipo de perfil,** seleccione **Plantillas** y elija entre las siguientes plantillas admitidas en Surface Hub:
   - Restricciones de dispositivos (Windows 10 Team), como se describe en la sección anterior.
   - Microsoft Defender para endpoint (Windows 10 Desktop)
   - Certificado PKCS
   - Certificado importado de PKCS
   - Certificado SCEP
   - Certificado de confianza

Crear perfil de configuración personalizado

Puede ampliar el ámbito de administración mediante la creación de un perfil personalizado mediante un URI de OMA desde cualquiera de los CSP admitidosen Microsoft Surface Hub . Cada configuración de un CSP tiene un OMA-URI correspondiente que puede establecer mediante perfiles de configuración personalizados en Intune. Para obtener información detallada sobre los SURFACE HUB, puede hacer referencia a los siguientes recursos:

- Referencia de proveedor de servicios de configuración
- CSP de directivas admitidas por Microsoft Surface Hub

- SurfaceHub CSP

> **NOTE**
> La administración de la cuenta del dispositivo mediante la configuración del CSP de SurfaceHub no es posible actualmente con Intune y requiere el uso de un proveedor MDM de terceros.

Para implementar la configuración de directiva basada en CSP, empiece generando un URI de OMA y, a continuación, agrégrelo a un perfil de configuración personalizado en Intune.

Generar URI de OMA para la configuración de destino

Para generar el URI de OMA para cualquier configuración:

1. En la documentación de CSP,identifique el nodo raíz del CSP. Por lo general, esto tiene el aspecto **./Vendor/MSFT/NameOfCSP**.
   - **Ejemplo:** El nodo raíz del CSP de SurfaceHub es **./Vendor/MSFT/SurfaceHub**.
2. Identificar la ruta de acceso del nodo para la configuración que quieras usar.
   - **Ejemplo:** La ruta de acceso de nodo para la configuración para habilitar la proyección inalámbrica es **InBoxApps/WirelessProjection/Enabled**.
3. Anexar la ruta de acceso del nodo raíz para generar el URI de OMA.
   - **Ejemplo:** El URI de OMA para la configuración para habilitar la proyección inalámbrica es **./Vendor/MSFT/SurfaceHub/InBoxApps/WirelessProjection/Enabled.**
4. El tipo de datos también se indica en la documentación de CSP. Los tipos de datos más comunes son:
   - char (Cadena)
   - int (Entero)
   - bool (Booleano)

Agregar URI de OMA al perfil de configuración personalizado

1. En Endpoint Manager, seleccione **Perfiles** > **de configuración de dispositivos Crear** > **perfil**.
2. En Plataforma, **seleccione Windows 10 y versiones posteriores.** En Perfil, seleccione **Personalizado**y, a continuación, **seleccione Crear.**
3. Agregue un nombre y una descripción opcional y, a continuación, **seleccione Siguiente.**
4. En **Configuración** > **OMA-URI Configuración**, seleccione **Agregar**.

Microsoft Teams y Skype Empresarial configuración

En esta sección se Teams y Skype Empresarial que puedes administrar a través de Intune u otro proveedor MDM. Esto incluye:

- Calidad del servicio (QoS)
- Administrar Teams características específicas del usuario

Configuración de calidad del servicio

Para garantizar una calidad óptima de vídeo y audio en Surface Hub, agrega la siguiente configuración de QoS al dispositivo.

NOMBRE	DESCRIPCIÓN	OMA-URI	TIPO	VALOR
Puertos de audio	Rango de puertos de audio	./Device/Vendor/MSFT/NetworkQoSPolicy/Audio/SourcePortMatchCondition	Cadena	50000-50019

NOMBRE	DESCRIPCIÓN	OMA-URI	TIPO	VALOR
DSCP de audio	Marcado de puertos de audio	./Device/Vendor/MSFT/NetworkQoSPolicy/Audio/DSCPAction	Integer	46
Puertos de vídeo	Rango de puertos de vídeo	./Device/Vendor/MSFT/NetworkQoSPolicy/Video/SourcePortMatchCondition	Cadena	50020-50039
DSCP de vídeo	Marcado de puertos de vídeo	./Device/Vendor/MSFT/NetworkQoSPolicy/Video/DSCPAction	Integer	34
Puertos de uso compartido	Intervalo de puertos compartidos	./Device/Vendor/MSFT/NetworkQoSPolicy/Sharing/SourcePortMatchCondition	Cadena	50040-50059
Uso compartido de DSCP	Marcado de puertos compartidos	./Device/Vendor/MSFT/NetworkQoSPolicy/Sharing/DSCPAction	Integer	18

> **NOTE**
> En la tabla se muestran los intervalos de puertos predeterminados. Los administradores pueden cambiar los intervalos de puertos en Skype Empresarial y en el panel de control de Teams.

Administrar Teams características específicas del usuario

Puede crear un perfil de configuración personalizado para administrar Teams reuniones coordinadas, la unión de proximidad y otras características. Para obtener más información, vea Manage Microsoft Teams configuration on Surface Hub.

Cambiar la aplicación predeterminada para las reuniones & llamadas

La aplicación predeterminada para reuniones & llamadas en el Surface Hub varía en función de cómo instales Windows 10 Team 2020 Update (también Windows 10 20H2 Team edition). Si vuelves a crear una imagen Surface Hub a Windows 10 20H2, Microsoft Teams se establecerá como el valor predeterminado, sin que Skype Empresarial esté disponible (modo 1). Si actualiza el concentrador desde una versión anterior del sistema operativo, Skype Empresarial permanecerá como predeterminado, con la funcionalidad Teams disponible (modo 0) a menos que ya haya configurado Teams como predeterminado.

Para cambiar la instalación predeterminada, use un perfil personalizado para establecer el Teams de reunión de la siguiente manera:

- Modo 0: Skype Empresarial con la funcionalidad de Microsoft Teams para reuniones programadas.
- Modo 1: Microsoft Teams solo.

NOMBRE	DESCRIPCIÓN	OMA-URI	TIPO	VALOR
Id. de aplicación de Teams	Nombre de la aplicación	./Vendor/MSFT/SurfaceHub/Properties/VtcAppPackageId	Cadena	Microsoft.MicrosoftTeamsforSurfaceHub_8wekyb3d8bbwe!Teams

NOMBRE	DESCRIPCIÓN	OMA-URI	TIPO	VALOR
Modo de aplicación de Teams	Modo Teams	./Vendor/MSFT/SurfaceHub/Properties/SurfaceHubMeetingMode	Integer	0 o 1

Configurar cuentas de administrador no globales en Surface Hub

12/01/2022 • 4 minutes to read

La actualización de Windows 10 Team 2020 agrega compatibilidad para configurar cuentas de administrador no globales que limiten los permisos a la administración de la aplicación Configuración en dispositivos Surface Hub unidos a un dominio de Azure AD. Esto le permite tener en cuenta los permisos de administración Surface Hub y evitar el acceso de administrador potencialmente no deseado en todo un dominio de Azure AD. Antes de comenzar, asegúrese de que el Surface Hub está unido a Azure AD e Intune autoinscribirse. Si no es así, tendrá que restablecer Surface Hub y completar el programa de instalación de la primera vez y sin necesidad de usar (OOBE), eligiendo la opción de unirse a Azure AD.

Resumen

El proceso de creación de cuentas de administración no globales implica los siguientes pasos:

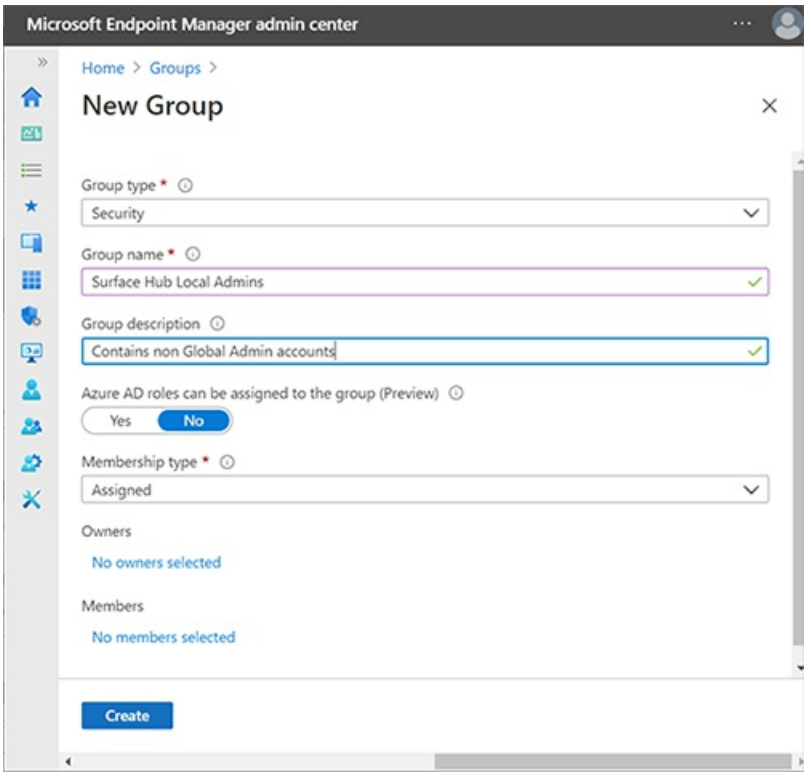
1. En Microsoft Intune, cree un grupo de seguridad que contenga los administradores designados para administrar Surface Hub.
2. Obtener SID de grupo de Azure AD con PowerShell.
3. Cree un archivo XML que contenga sid de grupo de Azure AD.
4. Cree un grupo de seguridad que contenga los Surface Hub que administrará el grupo seguridad de administradores no globales.
5. Crea un perfil de configuración personalizado destinado al grupo de seguridad que contiene los Surface Hub dispositivos.

Crear grupos de seguridad de Azure AD

En primer lugar, cree un grupo de seguridad que contenga las cuentas de administrador. A continuación, cree otro grupo de seguridad para Surface Hub dispositivos.

Crear grupo de seguridad para cuentas de administrador

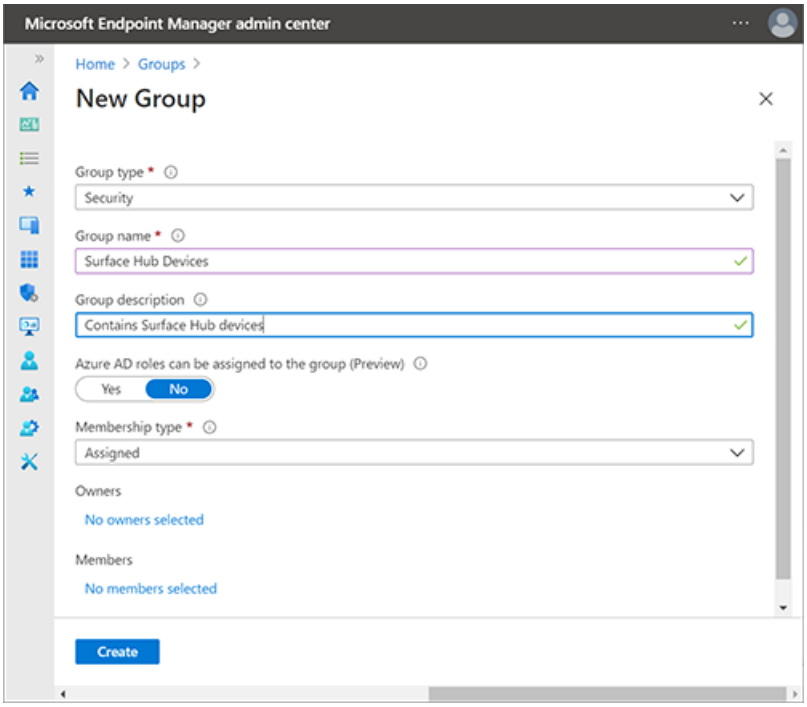
1. Inicie sesión en Intune a través Microsoft Endpoint Manager centrode administración, seleccione Grupos nuevos grupos > y, en Tipo de **** > **** grupo, seleccione **Seguridad.**
2. Escriba un nombre de grupo (por ejemplo, **Surface Hub administradores locales)** y, a continuación, **seleccione Crear.**



3. Abra el grupo, seleccione **Miembros**y, a continuación, elija Agregar miembros para especificar las cuentas de administrador que desea designar como administradores no globales en Surface Hub. **** Para obtener más información sobre cómo crear grupos en Intune, consulte Agregar grupos para organizar usuarios y dispositivos.

Crear grupo de seguridad para Surface Hub dispositivos

1. Repita el procedimiento anterior para crear un grupo de seguridad independiente para dispositivos concentradores; por ejemplo, **Surface Hub dispositivos**.



Obtener SID de grupo de Azure AD con PowerShell

1. Inicie PowerShell con privilegios de cuenta elevados (**Ejecutar**como administrador) y asegúrese de que el sistema está configurado para ejecutar scripts de PowerShell. Para obtener más información, consulte About Execution Policies.

2. Instalar Azure PowerShell módulo.

3. Inicie sesión en el inquilino de Azure AD.

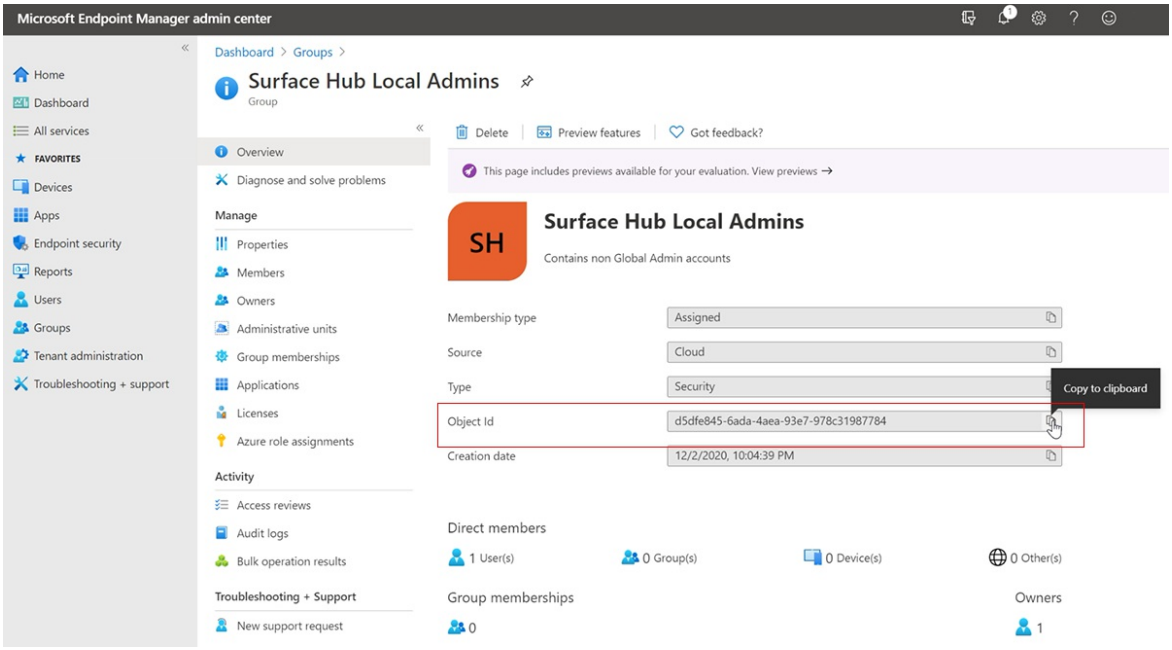
```
Connect-AzureAD
```

4. Cuando haya iniciado sesión en el inquilino, ejecute el siguiente commandlet. Se le pedirá que "Escriba el identificador de objeto de su grupo de Azure AD".

```
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. En Intune, seleccione el grupo que creó anteriormente y copie el identificador de objeto, como se muestra en la siguiente ilustración.



6. Ejecute el siguiente commandlet para obtener el SID del grupo de seguridad:

```
$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. Pegue el id. de objeto en el commandlet de PowerShell, presione **Entrar**y, a continuación, copie el **SID** de grupo de Azure AD en un editor de texto.

Crear archivo XML que contenga sid de grupo de Azure AD

1. Copie lo siguiente en un editor de texto:

```
<groupmembership>
<accessgroup desc = "S-1-5-32-544">
<member name = "Administrator" />
<member name = "S-1-12-1-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX" />
</accessgroup>
</groupmembership>
```

> **IMPORTANT**
>
> Es posible que deba usar el nombre localizado para la cuenta de administrador. No quite el miembro de administrador predeterminado del archivo XML.

2. Reemplace el SID de marcador de posición (empezando por S-1-12-1) por su **SID** de grupo de Azure AD y, a continuación, guarde el archivo como XML; por ejemplo, **aad-local-admin.xml**.

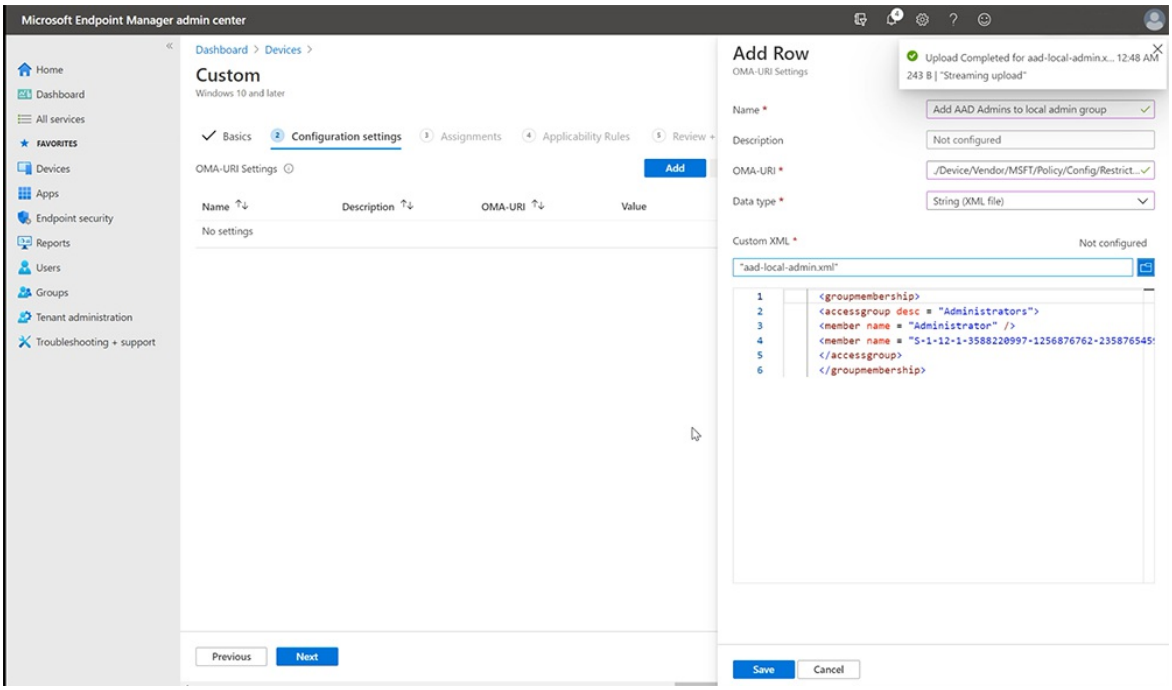
> **NOTE**
>
> Aunque los grupos deben especificarse a través de su SID, si desea agregar usuarios de Azure directamente, se pueden agregar especificando su nombre principal de usuario (UPN) en este formato:
> `<member name = "AzureAD\user@contoso.com" />`

Crear perfil de configuración personalizado

1. En Endpoint Manager, seleccione **Perfiles** > **de configuración de dispositivos Crear** > **perfil**.
2. En Plataforma, **seleccione Windows 10 y versiones posteriores.** En Perfil, seleccione **Personalizado**y, a continuación, **seleccione Crear.**
3. Agregue un nombre y una descripción y, a continuación, **seleccione Siguiente.**
4. En **Configuración** > **OMA-URI Configuración**, seleccione **Agregar**.
5. En el panel Agregar fila, agregue un nombre y, en **OMA-URI,** agregue la siguiente cadena:

```
./Device/Vendor/MSFT/Policy/Config/RestrictedGroups/ConfigureGroupMembership
```

6. En Tipo de datos, seleccione **String XML** y busque para abrir el archivo XML que creó en el paso anterior.



7. Haz clic en **Guardar**.
8. Haga **clic en Seleccionar grupos para incluir** y elegir el grupo de seguridad que creó anteriormente (Surface Hub**dispositivos**). Haz clic en **Siguiente**.
9. En Reglas de aplicabilidad, agregue una regla si lo desea. De lo contrario, **seleccione Siguiente** y, a continuación, **seleccione Crear**.

Para obtener más información sobre los perfiles de configuración personalizados con cadenas OMA-URI, vea Usar la configuración personalizada para Windows 10 dispositivos en Intune.

Administradores no globales que administran Surface Hub

Los miembros del **Surface Hub seguridad** de administradores locales ahora pueden iniciar sesión en la aplicación Configuración en Surface Hub y administrar la configuración.

> **IMPORTANT**
>
> Se quita el acceso predeterminado de los administradores globales a Configuración aplicación (a menos que también sean miembros de este nuevo grupo de seguridad).

Supervisar Microsoft Surface Hub

12/01/2022 • 2 minutes to read

La supervisión de dispositivos Microsoft Surface Hub está habilitada a través de Azure Monitor (anteriormente Microsoft Operations Management Suite o OMS). Para empezar, consulta Supervisar Surface Hubs con Azure Monitor para realizar un seguimiento de su estado.

Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Administrar actualizaciones de Windows en Surface Hub

12/01/2022 • 7 minutes to read

Las nuevas versiones del sistema operativo de Surface Hub se publican a través de Windows Update, igual que las versiones de Windows 10. Esta página explica los procedimientos recomendados para administrar actualizaciones de dispositivos Surface Hub.

Windows Update para empresas

Windows Update para empresas es un conjunto de características diseñadas para proporcionar a las empresas un control adicional sobre cómo y cuándo instala Windows Update las versiones, a la vez que reduce los costos de administración de dispositivos. Con este método, los Surface Hubs están conectados directamente al servicio Windows Update de Microsoft.

- Recibir actualizaciones directamente del servicio Windows Update de Microsoft, sin ninguna infraestructura adicional necesaria.
- Aplazar actualizaciones para proporcionar más tiempo para pruebas y evaluaciones.
- Implementar actualizaciones para seleccionar grupos de dispositivos.
- Definir ventanas de mantenimiento para instalar actualizaciones.

> **TIP**
> Usar el uso compartido de contenido de punto a punto para reducir los problemas de ancho de banda durante las actualizaciones. Consulta Optimizar la distribución de actualizaciones de Windows10 para obtener más información.

> **NOTE**
> Surface Hub no admite actualmente revertir las actualizaciones.

Modelo de mantenimiento de Surface Hub

Surface Hub usa el modelo de mantenimiento de Windows 10, que se denomina Windows como servicio (WaaS). Tradicionalmente, las nuevas características se agregan solo en las nuevas versiones de Windows que se publican cada pocos años. Cada nueva versión requiere implementar procesos largos y costosos en una organización. Como resultado, los usuarios finales y las organizaciones no suelen disfrutar de las ventajas de las nuevas innovaciones. El objetivo de Windows como servicio es proporcionar continuamente nuevas funcionalidades y mantener al mismo tiempo un alto nivel de calidad.

Microsoft publica dos tipos de versiones de Surface Hub ampliamente de manera continua:

- **Actualizaciones de características** - Actualizaciones que instalan las funciones, experiencias y capacidades nuevas más recientes. Microsoft espera publicar dos nuevas actualizaciones de características por año.
- **Actualizaciones de calidad** - Actualizaciones que se centran en la instalación de revisiones de seguridad, controladores y otras actualizaciones de mantenimiento. Microsoft espera publicar una actualización de calidad acumulativa cada mes.

A fin de mejorar la calidad de las versiones y simplificar las implementaciones, todas las nuevas versiones que Microsoft publique para Windows 10, incluidas las de Surface Hub, serán acumulativas. Esto significa que las nuevas actualizaciones de características y de calidad incluirán las cargas de todas las versiones anteriores (de forma optimizada para reducir los requisitos de almacenamiento y de redes) y la instalación de la versión en un dispositivo hará que este esté totalmente actualizado. Además, a diferencia de las versiones anteriores de Windows, no puedes instalar un subconjunto del contenido de una actualización de calidad de Windows 10. Por ejemplo, si una actualización de calidad incluye correcciones para tres vulnerabilidades de seguridad y un problema de confiabilidad, la implementación de la actualización dará como resultado la instalación de las cuatro correcciones.

El sistema operativo de Surface Hub recibe actualizaciones en el Canal semianual. Al igual que otras ediciones de Windows 10, el período de duración de mantenimiento es finito. Debes instalar actualizaciones de nuevas características en equipos que ejecuten estas ramas para seguir recibiendo actualizaciones de calidad.

Para obtener más información acerca de Windows como servicio, consulta Información general de Windows como servicio.

Usar Windows Update para empresas

Surface Hubs, como todos los dispositivos Windows 10, incluye **Windows Update para empresas (WUfB)** que te permite controlar cómo se actualizan los dispositivos. Windows Update para empresas ayuda a reducir los costos de administración de dispositivos y ofrece el control sobre la implementación de actualizaciones, así como acceso rápido a actualizaciones de seguridad y a las últimas innovaciones de Microsoft de manera continua. Para obtener más información, consulta Administrar actualizaciones con Windows Update para empresas.

Para configurar Windows Update para empresas:

1. Agrupar Surface Hub en anillos de implementación
2. Configurar cuándo recibe actualizaciones Surface Hub.

> **NOTE**
> Puede usar Microsoft Intune, Microsoft Endpoint Configuration Manager o un proveedor de MDM de terceros compatible para configurar WUfB. Tutorial: usar Microsoft InTune para configurar Windows Update para empresas.

Agrupar Surface Hub en anillos de implementación

Usa anillos de implementación para controlar cuándo se lanzan las actualizaciones para tus Surface Hubs, dándote tiempo para que las valides. Por ejemplo, puedes actualizar un grupo reducido de dispositivos para comprobar la calidad antes de realizar un lanzamiento general en tu organización. En función de quién administre Surface Hub en tu organización, considera la posibilidad de incorporar Surface Hub en los anillos de implementación generados para tus otros dispositivos Windows 10. Para obtener más información acerca de los anillos de implementación, consulta Generar anillos de implementación para las actualizaciones de Windows10.

Consulte la tabla siguiente para obtener ejemplos de anillos de implementación.

ANILLO DE IMPLEMENTACIÓN	TAMAÑO DEL ANILLO	RAMA DE MANTENIMIENTO	APLAZAMIENTO PARA ACTUALIZACIONES DE CARACTERÍSTICAS	APLAZAMIENTO PARA ACTUALIZACIONES DE CALIDAD (REVISIONES DE SEGURIDAD, CONTROLADORES Y OTRAS ACTUALIZACIONES)	PASO DE VALIDACIÓN
Versión preliminar (por ejemplo, dispositivos de prueba o que no sean imprescindibles)	Pequeña	Windows Insider Preview	Ninguno.	Ninguno.	Probar y evaluar la nueva funcionalidad manualmente. Pausar actualizaciones si hay problemas.
Versión publicada (por ejemplo, los dispositivos que usan equipos seleccionados)	Media	Canal semianual	Ninguno.	Ninguno.	Supervisar uso de dispositivos y comentarios de los usuarios. Pausar actualizaciones si hay problemas.
Implementación general (por ejemplo, la mayoría de los dispositivos de la organización)	Grande	Canal semianual	120 días después del lanzamiento.	7-14 días después del lanzamiento.	Supervisar uso de dispositivos y comentarios de los usuarios. Pausar actualizaciones si hay problemas.
Crítica (por ejemplo, los dispositivos en salas de reuniones de ejecutivos)	Pequeña	Canal semianual	180 días después del lanzamiento (aplazamiento máximo para actualizaciones de características).	30 días después del lanzamiento (aplazamiento máximo para actualizaciones de calidad).	Supervisar uso de dispositivos y comentarios de los usuarios.

Configurar cuándo recibe actualizaciones Surface Hub

Cuando hayas determinado los anillos de implementación para los Surface Hubs, configura directivas de aplazamiento de las actualizaciones para cada anillo:

- Para aplazar las actualizaciones de características, establece una directiva Update/DeferFeatureUpdatesPeriodInDays para cada anillo.
- Para aplazar actualizaciones de calidad, establece una directiva Update/DeferQualityUpdatesPeriodInDays para cada anillo.

> **NOTE**
> Si se producen problemas durante el lanzamiento de las actualizaciones, puedes pausarlas mediante Update/PauseFeatureUpdates y Update/PauseQualityUpdates.

Si usas un servidor proxy u otro método para bloquear las direcciones URL

Agregue las siguientes direcciones URL de sitios de confianza de Windows Update a la "lista de permitidos":

- `http(s)://*.update.microsoft.com`
- `http://download.windowsupdate.com`
- `http://windowsupdate.microsoft.com`

Una vez instalada la Actualización de aniversario de Windows 10 Team, puedes quitar estas direcciones para restablecer Surface Hub a su estado anterior.

Ventana de mantenimiento

Para garantizar que el dispositivo está siempre disponible para su uso durante las horas laborables, Surface Hub realiza sus funciones administrativas durante una ventana de mantenimiento especificada. Durante la ventana de mantenimiento, Surface Hub instala automáticamente las actualizaciones a través de Windows Update y reinicia el dispositivo 20 minutos antes del final de la ventana.

Surface Hub sigue estas directrices para aplicar las actualizaciones:

- Instala la actualización durante la siguiente ventana de mantenimiento. Si una reunión está programada para iniciarse durante el mantenimiento o si los sensores de Surface Hub detectan que se está usando el dispositivo, se pospondrá la actualización pendiente hasta la siguiente ventana de mantenimiento.
- Si la siguiente ventana de mantenimiento es después del período de gracia especificado de la actualización, el dispositivo calculará la siguiente ranura disponible durante las horas laborables usando el tiempo estimado de instalación a partir de los metadatos de la actualización. Continuará posponiendo la actualización si se ha programado una reunión o si los sensores de Surface Hub detectan que el dispositivo esté en uso.
- Si la siguiente ventana de mantenimiento **no** supera el período de gracia de la actualización, el Surface Hub seguirá pospuesto la actualización.
- Si se necesita reiniciar, el Surface Hub se reiniciará automáticamente durante la siguiente ventana de mantenimiento.

> **NOTE**
> Reserva tiempo para las actualizaciones cuando configures por primera vez tu Surface Hub. Por ejemplo, un trabajo pendiente de definiciones de virus puede estar disponible y deberá instalarse inmediatamente.

Se establece una ventana de mantenimiento predeterminada para todos los Surface Hubs nuevos:

- **Hora de Inicio:** 2:00 AM
- **Duración:** 2 horas

Para cambiar manualmente la ventana de mantenimiento:

1. Abre **Configuración** en tu Surface Hub.
2. Ve a **Actualización y seguridad** > **Windows Update** > **Opciones avanzadas**.
3. En **Horas de mantenimiento**, selecciona **Cambiar**.

Para cambiar la ventana de mantenimiento con MDM, establezca el nodo **MaintenanceHoursSimple** en el proveedor de servicio de configuración de SurfaceHub. Consulta Administrar la configuración con un proveedor de MDM para obtener más información.

Más información

- Entrada de blog: mantenimiento, vuelo y administración de actualizaciones de Surface Hub (con Intune, por

supuesto)

Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Administrar la configuración de Surface Hub

12/01/2022 • 2 minutes to read

En esta sección

TEMA	DESCRIPCIÓN
Administración local para la configuración de Surface Hub	Obtén información sobre la configuración de Surface Hub.
Accesibilidad	La configuración de accesibilidad para Surface Hub se puede cambiar mediante la aplicación Configuración. La encontrarás en Accesibilidad. Surface Hub tiene las mismas opciones de accesibilidad que Windows10.
Cambiar la cuenta del dispositivo de Surface Hub	Puedes cambiar la cuenta del dispositivo en Configuración para agregar una cuenta si no había ya una aprovisionada o para cambiar las propiedades de una cuenta que ya estaba aprovisionada.
Restablecimiento del dispositivo	Es posible que tengas que restablecer Surface Hub.
Usar el nombre de dominio completo con Surface Hub	Opciones para configurar el nombre de dominio con Surface Hub.
Administración de la red inalámbrica	Surface Hub ofrece dos opciones de conectividad de red a la red corporativa y a Internet: inalámbrica y con cable. Si bien ambas proporcionan acceso a la red, te recomendamos usar una conexión por cable.

Administración local para la configuración de Surface Hub

12/01/2022 • 4 minutes to read

Tras la configuración inicial de Microsoft Surface Hub, la configuración del dispositivo se puede administrar localmente mediante **Configuración**.

Configuración de Surface Hub

Los Surface Hubs tienen muchas opciones que son comunes a otros dispositivos Windows, pero también tienen opciones de configuración que solo se pueden configurar en los Surface Hubs. En esta tabla se enumeran las opciones de configuración que solo son configurables en los Surface Hubs.

VALOR	UBICACIÓN	DESCRIPCIÓN
Cuenta del dispositivo	Surface Hub > Cuentas	Establecer o cambiar la cuenta del dispositivo de Surface Hub.
Estado de sincronización de la cuenta del dispositivo	Surface Hub > Cuentas	Comprobar el estado de la sincronización del correo electrónico y el calendario de la cuenta del dispositivo en Surface Hub.
Rotación de contraseñas	Surface Hub > Cuentas	Elegir si se permite que el Surface Hub rote automáticamente la contraseña de la cuenta del dispositivo.
Cambiar la contraseña de la cuenta de administrador	Surface Hub > Cuentas	Cambiar la contraseña de la cuenta de administrador local. Esta característica solo está disponible si has configurado el dispositivo para usar un administrador local durante la primera ejecución.
Administración del dispositivo	Surface Hub > Administración de dispositivos	Administrar las directivas y aplicaciones empresariales mediante la administración de dispositivos móviles (MDM).
Paquetes de aprovisionamiento	Surface Hub > Administración de dispositivos	Establecer o cambiar los paquetes de aprovisionamiento instalados en el Surface Hub.
Abrir la aplicación Microsoft Store	Surface Hub > Aplicaciones y características	La aplicación Microsoft Store solo está disponible para los administradores a través de la aplicación Configuración.
Nombre de dominio de Skype Empresarial	Surface Hub > Llamadas y audio	Configurar un nombre de dominio de tu Skype Empresarial Server.

VALOR	UBICACIÓN	DESCRIPCIÓN
Volumen de altavoz predeterminado	Surface Hub > Llamadas y audio	Configurar el volumen del altavoz predeterminado para el Surface Hub cuando se inicia una sesión.
Configuración predeterminada de micrófono y altavoces	Surface Hub > Llamadas y audio	Configurar un micrófono y un altavoz predeterminados para las llamadas y un altavoz predeterminado para la reproducción de contenido multimedia.
Habilitar Dolby Audio X2	Surface Hub > Llamadas y audio	Configurar las mejoras de altavoces Dolby Audio X2.
Abrir la aplicación Conectar automáticamente	Surface Hub > Proyección	Elegir si la proyección abrirá automáticamente la aplicación Conectar o si debe esperar a la entrada del usuario antes de abrirla.
Desactivar la proyección inalámbrica con Miracast	Surface Hub > Proyección	Elegir si los moderadores pueden proyectar de forma inalámbrica en Surface Hub con Miracast.
Requerir un PIN para la proyección inalámbrica	Surface Hub > Proyección	Elegir si los contactos tienen que escribir un PIN antes de usar la proyección inalámbrica.
Canal de proyección inalámbrica (Miracast)	Surface Hub > Proyección	Establecer el canal para la proyección de Miracast.
Información de la reunión que se muestra en la pantalla de inicio de sesión	Surface Hub > Pantalla de inicio de sesión	Elegir si el organizador de la reunión, la hora y el asunto se mostrarán en la pantalla de inicio de sesión.
Fondo de pantalla de inicio de sesión	Surface Hub > Pantalla de inicio de sesión	Elija una imagen que se usará como fondo durante las sesiones de usuario y en la pantalla de bienvenida.
Tiempo de espera de sesión a la pantalla de bienvenida	Surface Hub > de & sesión	Elegir cuánto tiempo hasta que Surface Hub vuelve a la pantalla de inicio después de que no se detecte ningún movimiento.
Reanudar la sesión	Surface Hub > de & sesión	Elegir si se debe permitir que los usuarios reanuden la sesión después de que no se detecté ningún movimiento o limpiar automáticamente una sesión.
Acceso a archivos y reuniones de Office 365	Surface Hub > de & sesión	Elige si un usuario puede iniciar sesión en Office 365 para acceder a sus reuniones y archivos.
Activar la pantalla con sensores de movimiento	Surface Hub > de & sesión	Elegir si la pantalla se activa cuando se detecte movimiento.

VALOR	UBICACIÓN	DESCRIPCIÓN
Tiempo de espera de pantalla	Surface Hub > de & sesión	Elige cuánto tiempo debe estar inactivo el dispositivo antes de desactivar la pantalla.
Tiempo de espera de suspensión	Surface Hub > de & sesión	Elegir cuánto tiempo el dispositivo debe estar inactivo antes de pasar al modo de suspensión.
Nombre descriptivo	Surface Hub > Acerca de	Establecer el nombre del Surface Hub que los contactos verán al conectarse de forma inalámbrica.
Horas de mantenimiento	Actualización y seguridad > Windows Update > Opciones avanzadas	Configurar cuando se pueden instalar actualizaciones.
Recuperar desde la nube	Actualización y seguridad > Recuperación	Reinstalar el sistema operativo en Surface Hub a una compilación del fabricante desde la nube.
Guardar la clave de BitLocker	Actualización y seguridad > Recuperación	Hacer copia de seguridad de la clave de BitLocker de tu Surface Hub en una unidad USB.
Recopilar registros	Actualización y seguridad > Recuperación	Guardar los registros en una unidad USB para enviar a Microsoft más adelante.

Temas relacionados

Administrar la configuración de Surface Hub

Administración remota de Surface Hub

Guía del administrador de Microsoft Surface Hub

Administración de contraseñas (Surface Hub)

12/01/2022 • 2 minutes to read

Cada cuenta del dispositivo de Microsoft Surface Hub requiere una contraseña para autenticarse y habilitar características en el dispositivo. Por motivos de seguridad, es posible que quieras cambiar (o "rotar") esta contraseña con regularidad. Sin embargo, si la contraseña de la cuenta del dispositivo cambia, la contraseña que estaba almacenada en el dispositivo Surface Hub no será válida y se deshabilitarán todas las características que dependan de dicha cuenta del dispositivo. Tendrás que actualizar la contraseña de la cuenta del dispositivo en el Surface Hub desde la aplicación Configuración para volver a habilitar estas características.

Para simplificar la administración de contraseñas de las cuentas de dispositivo de Surface Hub, hay dos opciones:

1. Desactivar la expiración de la contraseña para la cuenta del dispositivo.
2. Permitir que el dispositivo Surface Hub rote automáticamente la contraseña de la cuenta del dispositivo.

Desactivar la rotación de contraseñas para la cuenta del dispositivo.

Establece la propiedad **PasswordNeverExpires** de la cuenta del dispositivo en True. Deberías comprobar si se cumplen los requisitos de seguridad de la organización.

Permitir que el Surface Hub rote automáticamente la contraseña de la cuenta del dispositivo

El Surface Hub puede cambiar automáticamente la contraseña de una cuenta de dispositivo sin necesidad de actualizarla manualmente. Puede habilitar esta característica en **Configuración** > **Surface Hub** > **Cuentas**. Si activa la rotación de contraseñas, Surface Hub intentará cambiar la contraseña cada 7 días durante el horario de mantenimiento. Las contraseñas no cambian durante una reunión. Si han transcurrido 7 días desde la última rotación de contraseña, pero el Surface Hub estaba desactivado, intentará cambiar la contraseña inmediatamente cuando se haya activado o cada 10 minutos hasta que se haya realizado correctamente.

Las contraseñas generadas automáticamente contienen de 15 a 32 caracteres, incluida una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Ten en cuenta que cuando se cambie la contraseña de la cuenta del dispositivo, no se mostrará la nueva contraseña. Si necesitas iniciar sesión en la cuenta o volver a proporcionar la contraseña (por ejemplo, si quieres cambiar la configuración de la cuenta de dispositivo en el Surface Hub), necesitarás usar Active Directory o el portal de administración de Microsoft 365 para restablecer la contraseña.

> **IMPORTANT**
>
> La opción de afiliación de dispositivos seleccionada durante la configuración inicial del Surface Hub tiene un impacto en el formato de cuenta del dispositivo que se puede usar con el giro de contraseña. Los concentradores asociados con un Active Directory local solo pueden girar las contraseñas de las cuentas de dispositivo especificadas en **formato dominio\nombredeusuario**. Los concentradores asociados con un Azure Active Directory solo pueden girar las contraseñas de las cuentas de dispositivo especificadas en formato, pero solo si la cuenta es solo en la nube o si el dominio de AAD está configurado para la autenticación en la nube y la escritura de escritura de `username@domain.com` contraseñas.

Accesibilidad (Surface Hub)

12/01/2022 • 2 minutes to read

Microsoft Surface Hub tiene las mismas opciones de accesibilidad que Windows10.

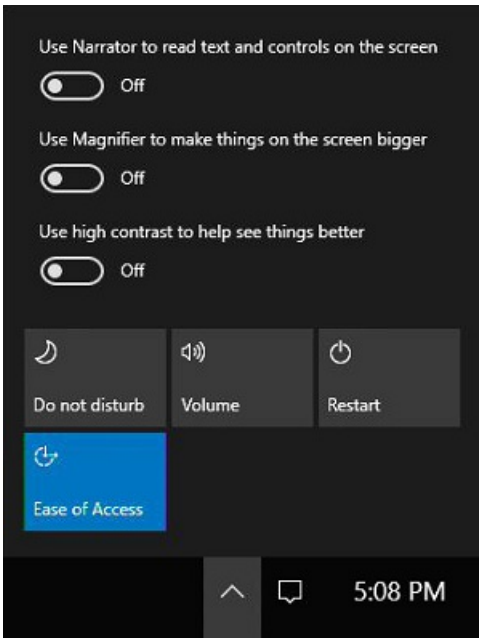
Configuración de accesibilidad predeterminada

La lista completa de la configuración de accesibilidad está disponible para los administradores de TI en la aplicación **Configuración**. La configuración de accesibilidad predeterminada de Surface Hub incluye:

CARACTERÍSTICA DE ACCESIBILIDAD	CONFIGURACIÓN PREDETERMINADA
Lupa	Desactivado
Contraste alto	Ningún tema seleccionado
Subtítulos	Valores predeterminados seleccionados para Fuente y Fondo y ventana
Teclado	El **teclado en pantalla**, las **teclas especiales**, las **teclas de alternancia**y las **teclas filtro** están desactivados.
Mouse	Valores predeterminados seleccionados para el **tamaño del puntero**, el **color del puntero** y las **teclas de mouse**.
Otras opciones	Valores predeterminados seleccionados para **Opciones visuales** e **Comentarios táctiles**.

La característica de accesibilidad Narrador no está disponible en la aplicación **Configuración**. De manera predeterminada, el Narrador está desactivado. Para cambiar la configuración predeterminada del Narrador, lleva a cabo los pasos con un teclado y mouse.

1. Descarta la pantalla de inicio de sesión.
2. Abre **Acciones rápidas** > **Accesibilidad** de la barra de estado.



3. Activa el Narrador.
4. Haz clic en **Conmutador de tareas**.
5. Selecciona **Configuración del Narrador** en Conmutador de tareas. Ahora puedes editar la configuración predeterminada de Narrador.

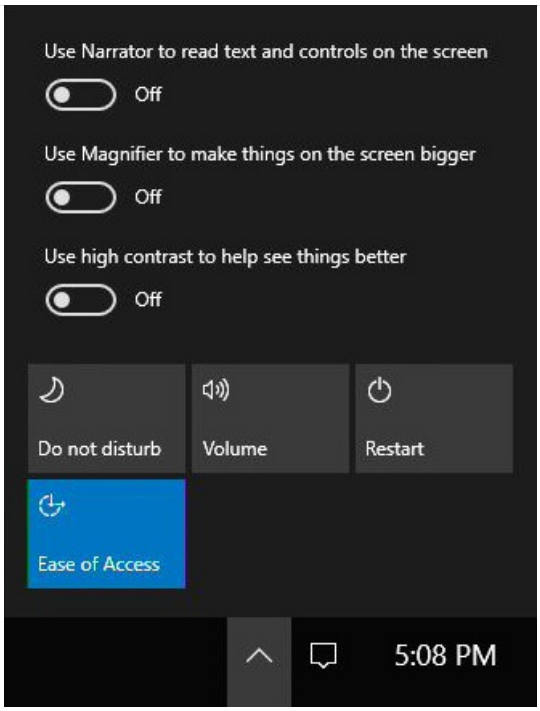
Además, estas aplicaciones y características de accesibilidad vuelven a la configuración predeterminada cuando los usuarios presionan Finalizar sesión:

- Narrador
- Lupa
- Contraste alto
- Teclas de filtro
- Teclas especiales
- Teclas de alternancia
- Teclas del mouse

Cambiar la configuración de accesibilidad durante una reunión

Durante una reunión, los usuarios pueden alternar las aplicaciones y las características de accesibilidad de un par de formas:

- Métodos abreviados de teclado
- **Acciones rápidas** > **Accesibilidad** de la barra de estado



Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Cambiar la cuenta del dispositivo de Microsoft Surface Hub.

12/01/2022 • 2 minutes to read

Puedes cambiar la cuenta del dispositivo en Configuración para agregar una cuenta si no había ya una aprovisionada o para cambiar las propiedades de una cuenta que ya estaba aprovisionada.

Detalles

VALOR	DESCRIPCIÓN
Nombre principal del usuario	El nombre principal de usuario (UPN) de la cuenta del dispositivo.
Contraseña	La contraseña correspondiente a la cuenta del dispositivo.
Dominio	El dominio al que pertenece la cuenta del dispositivo. Este campo no tiene que proporcionarse en las cuentas de Office 365.
Nombre de usuario	El nombre de usuario de la cuenta del dispositivo. Este campo no tiene que proporcionarse en las cuentas de Office 365.
Dirección de Protocolo de inicio de sesión (SIP)	La dirección SIP de la cuenta del dispositivo.
Servidor Microsoft Exchange	Este es el servidor Exchange de la cuenta del dispositivo. El nombre de usuario y la contraseña de la cuenta del dispositivo deben poder autenticarse en el servidor Exchange especificado.
Habilitar los servicios Exchange	Cuando estén activados, se habilitarán todos los servicios de Exchange (por ejemplo, el calendario en la pantalla de bienvenida y el envío de pizarras por correo electrónico). Si no están activados, se deshabilitarán todos los servicios de Exchange y no será necesario proporcionar el servidor Exchange.

Qué sucede

El UPN y la contraseña se usan para validar la cuenta en AD o Azure AD. Si se produce un error en la validación, deberás proporcionar el dominio y el nombre de usuario.

Una vez proporcionadas las credenciales, intentaremos detectar la dirección SIP. Si no se encuentra una

dirección SIP, Skype Empresarial usará el UPN como la dirección SIP. Si esta no es la dirección SIP de la cuenta, deberás proporcionar la dirección SIP.

Se deberá proporcionar la dirección del servidor Exchange si el dispositivo no puede encontrar un servidor asociado a las credenciales de inicio de sesión. Microsoft Surface Hub usará el servidor Exchange para comunicarse con ActiveSync, que habilita varias características clave en el dispositivo.

Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Configurar el nombre de dominio de Skype Empresarial

12/01/2022 • 2 minutes to read

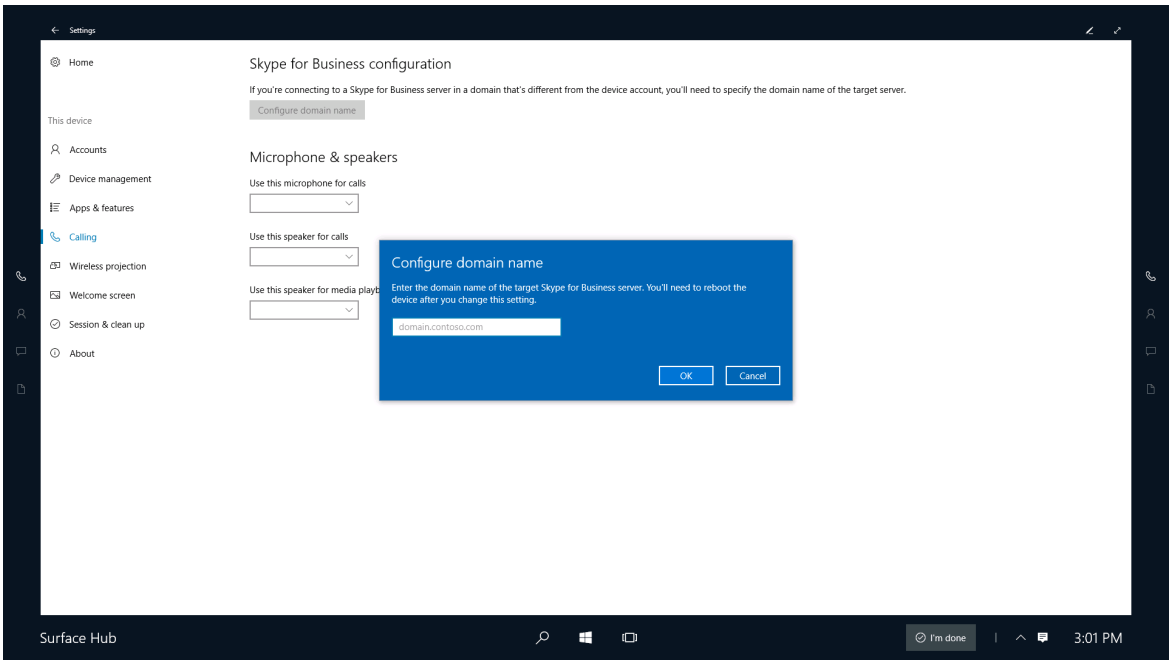
Existen algunos escenarios donde es necesario especificar el nombre de dominio del servidor de Skype Empresarial:

- **Varios sufijos DNS**: cuando tu infraestructura de Skype Empresarial tiene espacios de nombres inconexos como ese o más servidores tienen un sufijo DNS que no coincide con el sufijo de la dirección de inicio de sesión (SIP) para Skype Empresarial.
- **Los sufijos de Skype Empresarial y Exchange son diferentes**: cuando el sufijo de la dirección de inicio de sesión para Skype Empresarial es diferente al sufijo de la dirección de Exchange usada para la cuenta del dispositivo.
- **Trabajar con certificados:** las organizaciones grandes con servidores de Skype Empresarial locales usan normalmente certificados con su propia entidad de certificación raíz (CA). El dominio de entidad de certificación raíz suele ser diferente al dominio del servidor de Skype Empresarial, por lo que no se confía en el certificado y se produzca un error de inicio de sesión. Skype debe conocer el nombre de dominio del certificado para configurar una relación de confianza. Las empresas suelen usar directivas de grupo para insertarlo en el escritorio de Skype, pero la directiva de grupo no se admite en Surface Hub.

Para configurar el nombre de dominio de Skype Empresarial Server

1. En Surface Hub, abre **Configuración**.
2. Haz clic en **Surface Hub** y, a continuación, haz clic en **Llamadas y audio**.
3. En **Configuración de Skype Empresarial**, haz clic en **Configurar nombre de dominio**.
4. Escribe el nombre de dominio de tu servidor de Skype Empresarial y, después, haz clic en **Aceptar**.

> **TIP**
> Puedes escribir varios nombres de dominio separados por comas.
> Por ejemplo: 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

Administración de red inalámbrica (Surface Hub)

12/01/2022 • 2 minutes to read

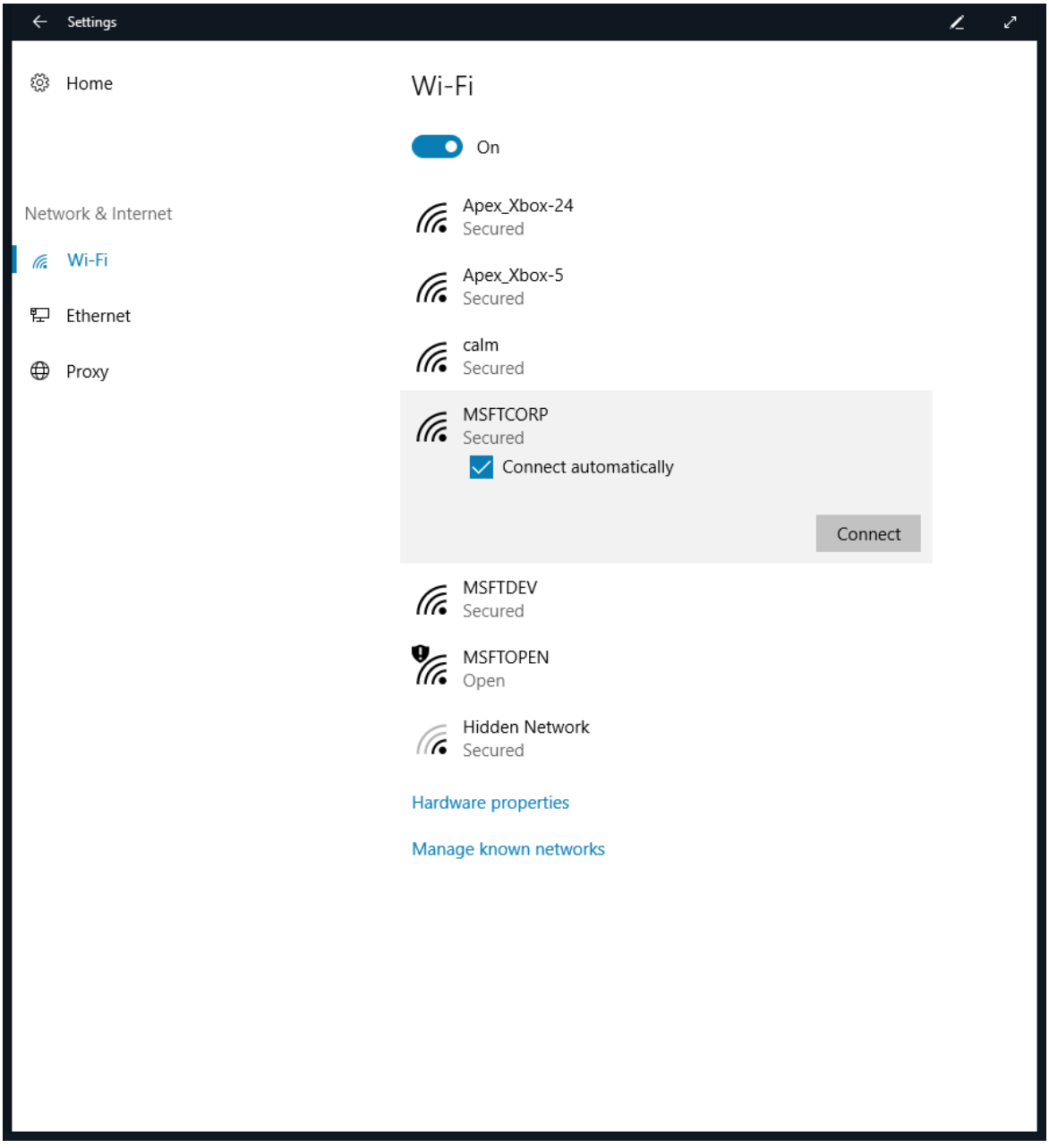
Microsoft Surface Hub ofrece dos opciones de conectividad de red a la red corporativa y a Internet: inalámbrica y con cable. Si bien ambas proporcionan acceso a la red, te recomendamos usar una conexión por cable.

Modificar, agregar o revisar una conexión de red

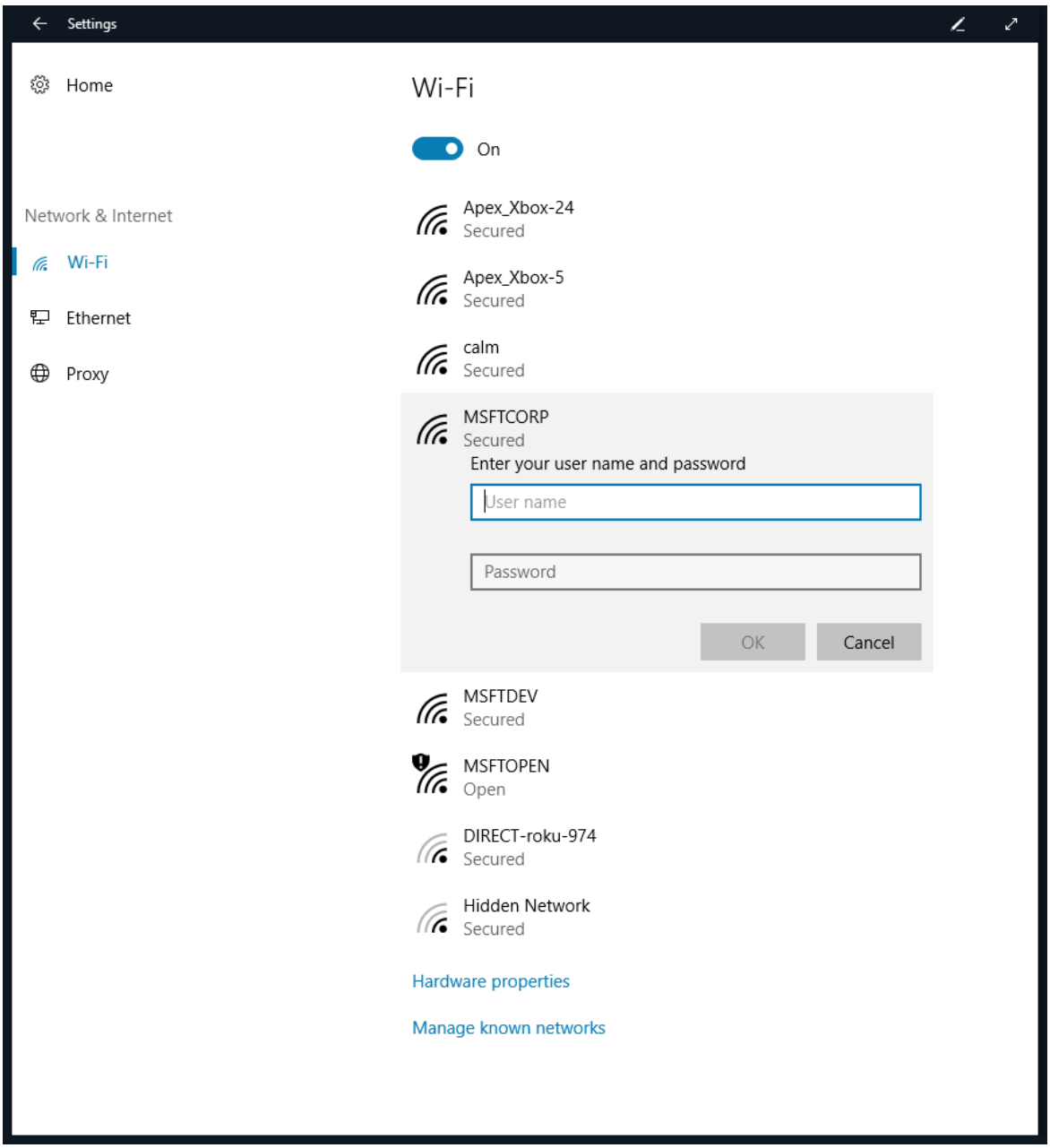
Si la conexión de red con cable no está disponible, el Surface Hub puede de usar una red inalámbrica para acceder a Internet. Debe haber un punto de acceso Wi-Fi conectado y configurado correctamente disponible y dentro del alcance del Surface Hub.

Elige un punto de acceso inalámbrico

1. En el Surface Hub, abre **Configuración** y escribe las credenciales de administrador.
2. Haz clic en **Red e Internet**. En **Wi-Fi**, elige un punto de acceso. Si quieres que Surface Hub se conecte automáticamente a este punto de acceso, haz clic en **Conectar automáticamente**. Haz clic en **Connect**.

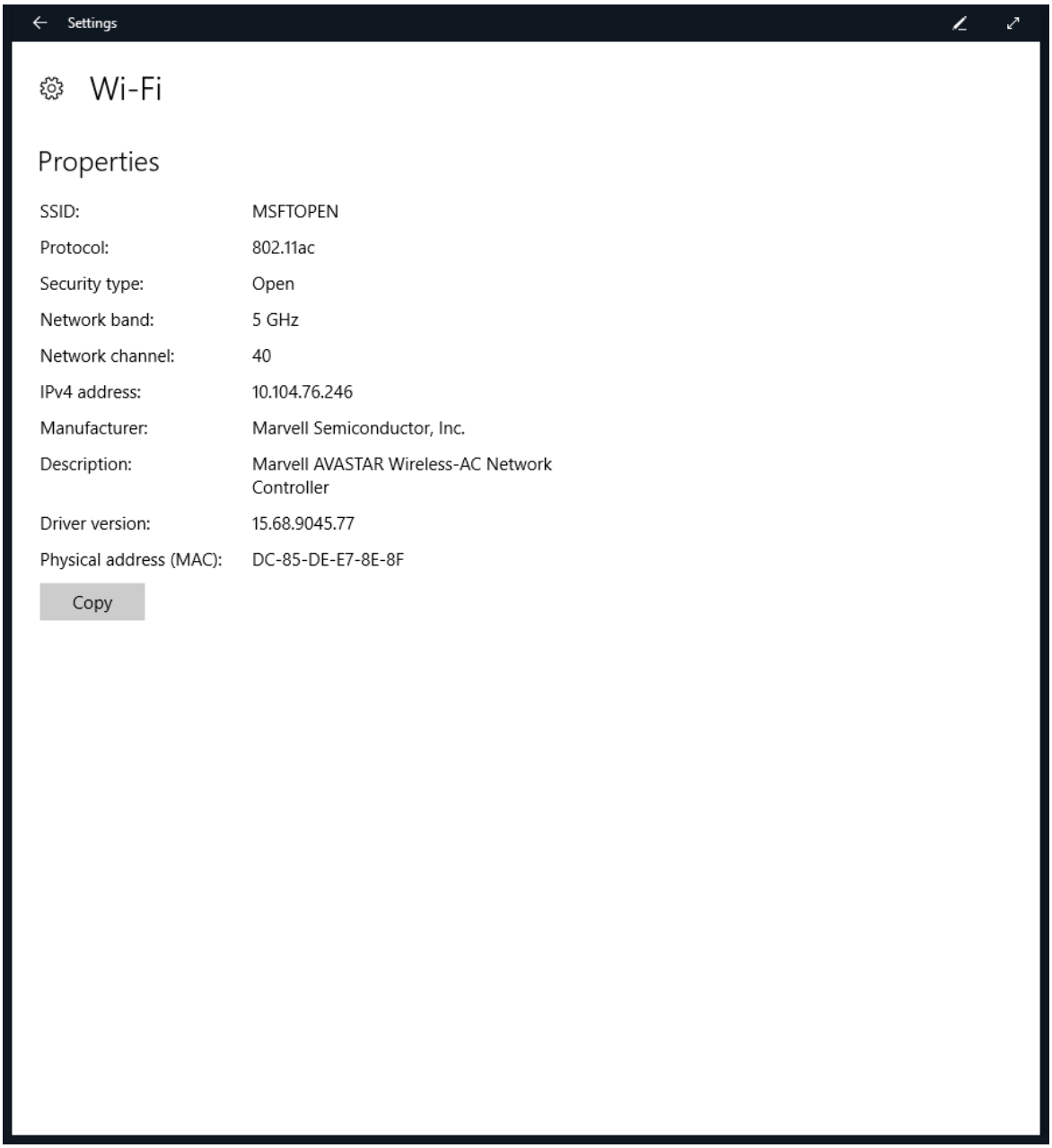


3. Si la red está protegida, se te pedirá que escribas la clave de seguridad. Haz clic en **Siguiente** para conectar.



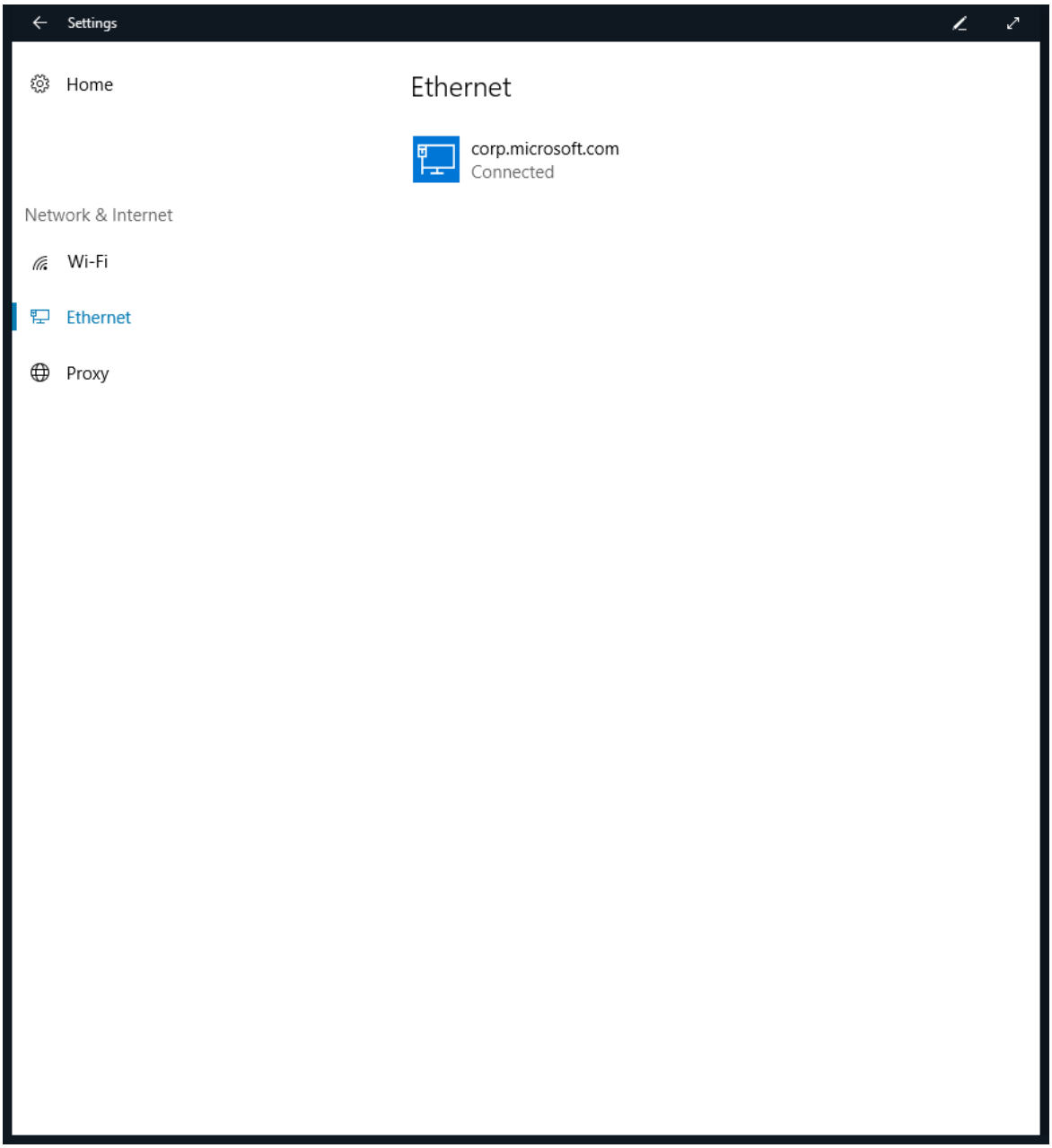
Revisa la configuración inalámbrica

1. En Surface Hub, abre **Configuración** y escribe las credenciales de administrador.
2. Haz clic en **Red e Internet**, luego en **Wi-Fi** y, a continuación, en **Opciones avanzadas**.
3. El Surface Hub te muestra las propiedades de la conexión de red inalámbrica.

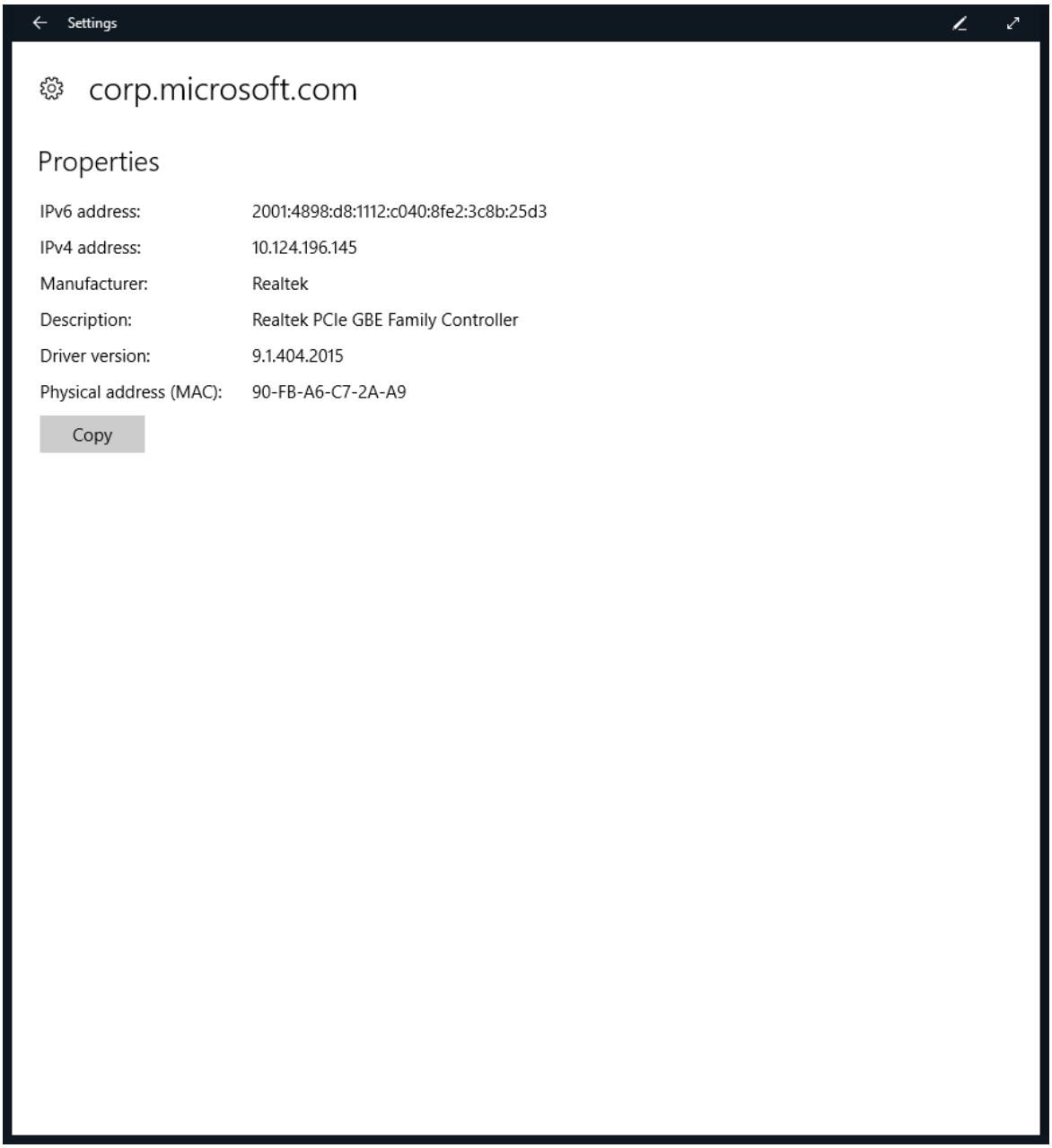


Revisar opciones de red por cable

1. En el Surface Hub, abre **Configuración** y escribe las credenciales de administrador.
2. Haz clic en **Sistema**, **Redes e Internet** y, a continuación, haz clic en la red en Ethernet.



3. El sistema te mostrará las propiedades de la conexión de red por cable.



Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Implementar calidad de servicio (QoS) en Surface Hub

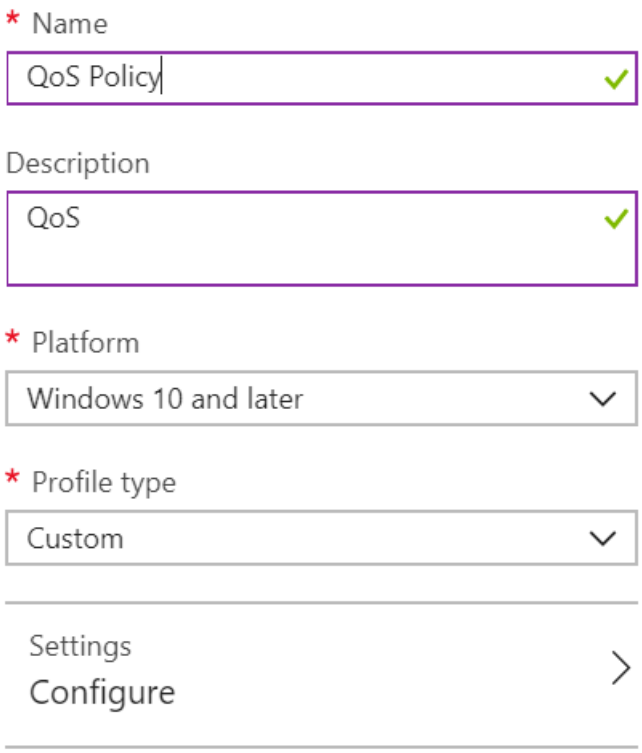
12/01/2022 • 2 minutes to read

Calidad de servicio (QoS) es una combinación de tecnologías de red que permite a los administradores optimizar la experiencia de comunicaciones de uso compartido de aplicaciones y audio en tiempo real.

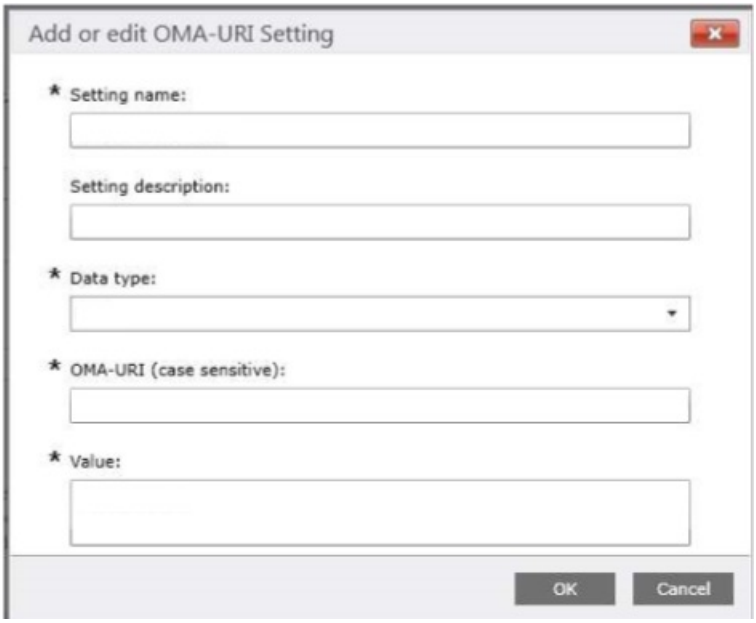
La configuración de QoS Skype Empresarial en el Surface Hub puede realizarse con el proveedor de administración de dispositivos móviles (MDM) o a través de un paquete de aprovisionamiento.

En este procedimiento se explica cómo configurar QoS para Surface Hub mediante Microsoft Intune.

1. En Intune, cree una directiva personalizada.



2. En **Custom OMA-URI Configuración**, seleccione **Agregar**. Para cada configuración que agregue, escribirá un nombre, una descripción (opcional), un tipo de datos, OMA-URI y un valor.



3. Agregue la siguiente configuración de OMA-URI personalizada:

NOMBRE	TIPO DE DATOS	OMA-URI ./DEVICE/VENDOR/MSFT/ NETWORKQOSPOLICY	VALOR
Puerto de origen de audio	Cadena	/HubAudio/SourcePortMatchCondition	Obtener los valores de su Skype administrador
DSCP de audio	Integer	/HubAudio/DSCPAction	46
Puerto de origen de vídeo	Cadena	/HubVideo/SourcePortMatchCondition	Obtener los valores de su Skype administrador
DSCP de vídeo	Integer	/HubVideo/DSCPAction	34
Nombre del proceso de audio	Cadena	/HubAudio/AppPathNameMatchCondition	Microsoft.PPISkype.Windows.exe
Nombre del proceso de vídeo	Cadena	/HubVideo/AppPathNameMatchCondition	Microsoft.PPISkype.Windows.exe

IMPORTANT

Cada **ruta de acceso de OMA-URI** comienza por `./Device/Vendor/MSFT/NetworkQoSPolicy`. La ruta de acceso completa para la configuración del puerto de origen de audio, por ejemplo, será `./Device/Vendor/MSFT/NetworkQoSPolicy/HubAudio/SourcePortMatchCondition`.

4. Cuando se haya creado la directiva, impleméntela en Surface Hub.

WARNING

Actualmente, no puede configurar la **configuración IPProtocolMatchCondition** en networkQoSPolicy CSP. Si esta configuración está configurada, la directiva no se aplicará.

Instalar aplicaciones en Microsoft Surface Hub

12/01/2022 • 7 minutes to read

Puedes instalar aplicaciones adicionales en tu Surface Hub para ajustarse a las necesidades de tu equipo u organización. Existen distintos métodos para instalar aplicaciones en función de si estás desarrollando y probando una aplicación o implementando una aplicación publicada. Este tema describe los métodos para instalar aplicaciones para cualquiera de esos escenarios.

Directrices de la aplicación admitidas

- Surface Hub solo puede ejecutar aplicaciones de la Plataforma universal de Windows (UWP). Las aplicaciones creadas con la herramienta de empaquetado MSIX no se ejecutarán en Surface Hub.
- Las aplicaciones deben elegirse para la familia de dispositivos universales o la familia de dispositivos del Equipo de Windows.
- Surface Hub solo admite aplicaciones con licencia sin conexión desde Microsoft Store para Empresas.
- De manera predeterminada, deben ser aplicaciones firmadas por la Store para poder instalarse. Durante la fase de desarrollo y prueba, también puedes elegir ejecutar aplicaciones para UWP firmadas por el desarrollador colocando el dispositivo en modo de desarrollador.
- Al enviar una aplicación al Microsoft Store, los desarrolladores deben establecer la disponibilidad de la familia de dispositivos y las opciones de licencias organizativas para asegurarse de que una aplicación estará disponible para ejecutarse en Surface Hub.
- Necesitas credenciales de administrador para instalar aplicaciones en el Surface Hub. Dado que el dispositivo está diseñado para usarse en espacios comunes como salas de reuniones, las personas no pueden acceder a la Microsoft Store para descargar e instalar aplicaciones.

Implementar aplicaciones publicadas

Hay varias opciones para la instalación de aplicaciones que se han publicado en la Microsoft Store en función de si quieres evaluarlas en algunos dispositivos o implementarlas ampliamente en tu organización.

Para instalar aplicaciones publicadas:

- Descarga la aplicación con la aplicación de la Microsoft Store, o
- Descarga el paquete de la aplicación de la Tienda Microsoft para Empresas y distribúyelo usando un paquete de aprovisionamiento o un proveedor de MDM compatible.

Aplicación de la Microsoft Store

Para evaluar aplicaciones publicadas de la Microsoft Store, usa la aplicación de la Microsoft Store en el Surface Hub para buscar y descargar aplicaciones.

> **NOTE**
> El uso de la aplicación de la Microsoft Store no es el método recomendado para implementar aplicaciones a escala en tu organización:
>
> - Para descargar aplicaciones, debes iniciar sesión en la aplicación de la Microsoft Store con una cuenta de Microsoft u organizativa. Sin embargo, solo puedes conectar una cuenta a un máximo de 10 dispositivos al mismo tiempo. Si tienes más de 10 Surface Hubs, deberás crear varias cuentas o quitar dispositivos de tu cuenta entre las instalaciones de las aplicaciones.
> - Para instalar aplicaciones, tendrás que iniciar sesión manualmente en la aplicación de la Microsoft Store en cada Surface Hub del que seas propietario.

Examinar la Microsoft Store en Surface Hub

1. En Surface Hub, inicia **Configuración**.
2. Escribe las credenciales de administrador del dispositivo cuando se solicite.
3. Vaya a **Surface Hub** > **aplicaciones & características**.
4. Selecciona **Abrir tienda** y busca la aplicación que estás buscando.

Descargar paquetes de la aplicación de la Tienda Microsoft para Empresas

Para descargar el paquete de la aplicación que necesitas para instalar aplicaciones en el Surface Hub, visita la Tienda Microsoft para Empresas. La Tienda para empresas es el lugar donde puedes buscar, comprar y administrar aplicaciones para los dispositivos Windows 10 de tu organización, incluido el Surface Hub.

> **NOTE**
> Actualmente, Surface Hub solo es compatible con aplicaciones con licencia sin conexión disponibles a través de la Tienda Microsoft para Empresas. Los desarrolladores de aplicaciones establecen la disponibilidad de la licencia sin conexión cuando envían las aplicaciones.

Busca y compra la aplicación que quieras y, a continuación, descarga:

- El paquete de la aplicación con licencia sin conexión (un .appx o un .appxbundle)
- El archivo de licencia *sin codificar* (si usas paquetes de aprovisionamiento para instalar la aplicación)
- La archivo de licencia *codificado* (si usas MDM para distribuir la aplicación)
- Los archivos de dependencia necesarios

Para obtener más información, consulta Descargar una aplicación con licencia sin conexión.

Instalar aplicaciones con licencia sin conexión a través del paquete de aprovisionamiento

Puedes instalar manualmente las aplicaciones con licencia sin conexión que hayas descargado de la Tienda para empresas en varios Surface Hubs mediante paquetes de aprovisionamiento. Usa Diseñador de imágenes y configuraciones de Windows (ICD) para crear un paquete de aprovisionamiento que contenga el paquete de la aplicación y el archivo de licencia *sin codificar* que descargaste de la Tienda para empresas. Para obtener más información, vea Create provisioning packages for Surface Hub.

Proveedor de MDM compatible

Para implementar aplicaciones en un gran número de Surface Hubs de tu organización, usa un proveedor de MDM compatible. La siguiente tabla muestra qué proveedores de MDM admiten la implementación de paquetes de aplicaciones con licencia sin conexión.

PROVEEDOR DE MDM	COMPATIBLE CON PAQUETES DE APLICACIONES CON LICENCIA SIN CONEXIÓN
MDM local con Configuration Manager (a partir de la versión 1602)	Sí
Proveedor de MDM de terceros	Comprueba que tu proveedor de MDM admite la implementación de paquetes de aplicaciones con licencia sin conexión.

NOTE

Para implementar aplicaciones sin conexión de forma remota mediante Microsoft Intune, consulte Manage VPP apps from Microsoft Store para Empresas. Surface Hub implementación de aplicaciones solo admite aplicaciones sin conexión que están asignadas a un grupo de dispositivos y usan el tipo de licencia Dispositivo.

Desarrollar y probar aplicaciones

En esta sección se proporciona información a los desarrolladores de aplicaciones para probar aplicaciones en Surface Hub.

Modo de desarrollador

De manera predeterminada, Surface Hub solo ejecuta aplicaciones para UWP que hayan sido publicadas y firmadas por la Microsoft Store. Las aplicaciones enviadas a la Microsoft Store se someten a pruebas de seguridad y cumplimiento como parte del proceso de certificación de la aplicación y esto permite proteger tu Surface Hub frente a aplicaciones malintencionadas.

Al habilitar el modo de desarrollador, también puedes instalar aplicaciones para UWP firmadas por el desarrollador.

IMPORTANT

Una vez habilitado el modo de desarrollador, deberás restablecer el Surface Hub para deshabilitarlo. Al restablecer el dispositivo se eliminan todas las configuraciones y los archivos de usuario locales y, a continuación, se vuelve a instalar Windows.

Activar el modo de desarrollador

1. En tu Surface Hub, inicia **Configuración**.
2. Escribe las credenciales de administrador del dispositivo cuando se solicite.
3. Navega hasta **Actualización y seguridad** > ** Para desarrolladores**.
4. Selecciona **Modo de desarrollador** y acepta la advertencia.

VisualStudio

Durante el desarrollo, la forma más sencilla de probar tu aplicación en un Surface Hub es usando Visual Studio. La característica de depuración remota de Visual Studio te ayuda a detectar problemas en tu aplicación antes de su implementación general. Para obtener más información, consulta Probar aplicaciones de Surface Hub con Visual Studio.

Crear paquete de aprovisionamiento

Usa Visual Studio para crear un paquete de la aplicación para tu aplicación para UWP, firmada mediante un certificado de prueba. A continuación, usa Diseñador de imágenes y configuraciones de Windows (ICD) para crear un paquete de aprovisionamiento que contenga el paquete de la aplicación. Para obtener más información,

vea Create provisioning packages for Surface Hub.

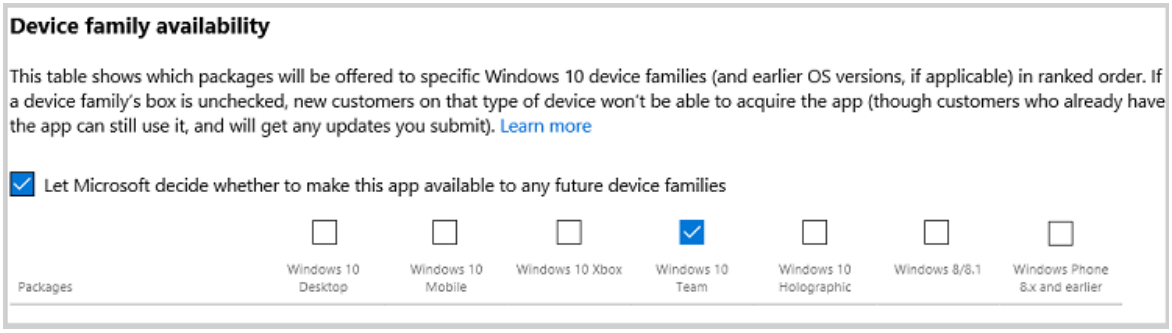
Enviar aplicaciones a la Microsoft Store

Cuando una aplicación está lista para publicarse, los desarrolladores necesitan enviarla y publicarla en la Microsoft Store. Para obtener más información, consulta Publicar Windows aplicaciones y juegos.

Durante el envío de la aplicación, los desarrolladores deben establecer la **disponibilidad de familias de dispositivos** y las opciones de **licencias de organización** para asegurarse de que la aplicación estará disponible para su ejecución en Surface Hub.

Establecer la disponibilidad de familias de dispositivos

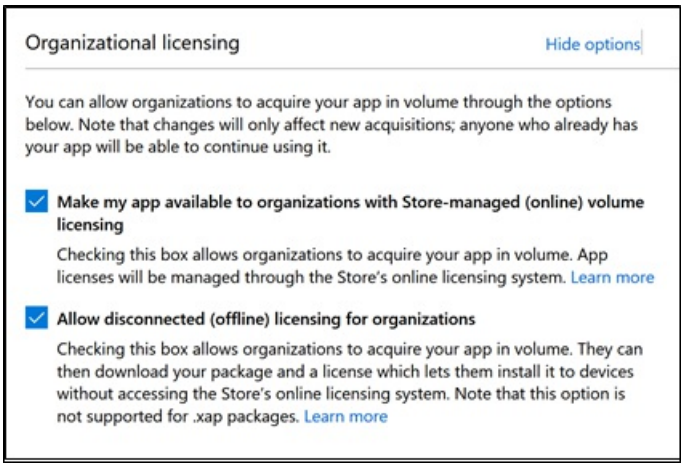
1. En el centro de desarrollo de Windows, ve a la página de envío de la aplicación.
2. Selecciona **Paquetes**.
3. En **Disponibilidad de familias de dispositivos**, selecciona estas opciones:
   - **Windows 10 Team**
   - **Permitir que Microsoft decida si quiere que la aplicación esté disponible para futuras familias de dispositivos**



Para obtener más información, consulta Disponibilidad de familias de dispositivos.

Establecer licencias de organización

1. En el centro de desarrollo de Windows, ve a la página de envío de la aplicación.
2. Selecciona **Precios y disponibilidad**.
3. En licencias de organización, selecciona **Permitir la compra de licencias en desconexión (sin conexión) para empresas**.



> **NOTE**
>
> **Hacer que mi aplicación esté disponible para organizaciones mediante la concesión de licencias administradas por Store (en línea) y distribución** está seleccionada de forma predeterminada.

> **NOTE**
>
> Los desarrolladores también pueden publicar aplicaciones de línea de negocio directamente en las empresas sin necesidad de que estén ampliamente disponibles en la Store. Para obtener más información, consulta Distribuir aplicaciones de LOB a empresas.

Para obtener más información, consulta Opciones de licencias de organización.

Resumen

Hay varias formas diferentes de instalar aplicaciones en tu Surface Hub según si estás desarrollando aplicaciones, evaluando aplicaciones en un número reducido de dispositivos o implementando aplicaciones de forma general en tu organización. En esta tabla se resumen los métodos admitidos:

MÉTODO DE INSTALACIÓN	DESARROLLO DE APLICACIONES	EVALUACIÓN DE APLICACIONES EN ALGUNOS DISPOSITIVOS	IMPLEMENTACIÓN DE APLICACIONES AMPLIAMENTE EN SU ORGANIZACIÓN
VisualStudio	X		
Paquete de aprovisionamiento	X	X	
Aplicación de la Microsoft Store		X	
Proveedor de MDM compatible			X

Configurar el menú Inicio de Surface Hub

12/01/2022 • 3 minutes to read

La actualización de 17 de enero de 2018 a Windows 10 (compilación 15063.877) permite menús Inicio personalizados en dispositivos Surface Hub. Aplica el diseño del menú Inicio personalizado usando administración de dispositivos móviles (MDM).

Al aplicar un diseño de menú Inicio personalizado a Surface Hub, los usuarios no pueden anclar, desanclar ni desinstalar aplicaciones desde Inicio.

Cómo aplicar un menú Inicio personalizado a Surface Hub

El menú Inicio personalizado se define en un archivo XML de diseño de Inicio. Tienes dos opciones para crear el archivo XML de diseño de Inicio:

- Editar el XML de Inicio de Surface Hub predeterminado

  O bien

- Configurar el menú Inicio deseado en un equipo de escritorio (anclando solo aplicaciones que estén disponibles en Surface Hub) y luego exportar el diseño.

> **TIP**
> Para agregar una ventana con un vínculo web al menú Inicio de escritorio, ve al vínculo en Microsoft Edge, selecciona `...` en la esquina superior derecha y selecciona **Anclar esta página a Inicio**. Consulta un diseño de Inicio que incluya un vínculo de Microsoft Edge para ver un ejemplo de cómo aparecerán los vínculos en el XML.

Para editar el XML predeterminado o el diseño exportado, familiarízate con el XML de diseño de Inicio. Hay unas pocas diferencias entre el diseño de Inicio en un escritorio y en Surface Hub.

Cuando tengas el menú Inicio definido en un XML de diseño de Inicio, crea una directiva MDM para aplicar el diseño.

Diferencias entre los menús Inicio de Surface Hub y de escritorio

Existen unas pocas diferencias clave entre la personalización del menú Inicio para Surface Hub y para un escritorio de Windows 10:

- No puede usar **DesktopApplicationTile en** el XML de diseño de inicio porque Windows aplicaciones de escritorio (Win32) no se admiten en Surface Hub.
- No puedes usar el XML de diseño de Inicio para configurar la barra de tareas o la pantalla de inicio de sesión de Surface Hub.
- La directiva de diseño de inicio solo debe asignarse a dispositivos, no a usuarios.
- La configuración de OMA-URI que se va a usar en la directiva es `./Device/Vendor/MSFT/Policy/Config/Start/StartLayout`
- Surface Hub admite un máximo de 6 columnas (6 ventanas 1 x 1); sin embargo, **debes** definir `GroupCellWidth=8` incluso aunque Surface Hub muestre solo ventanas de pantalla en las columnas 0 - 5, y no en las columnas 6 y 7.
- Surface Hub admite un número máximo de 6 filas (6 iconos de 1 x 1)

- `SecondaryTile`, que se usa para vínculos, que abrirán el vínculo en Microsoft Edge.

Ejemplo: Diseño de Inicio de Surface Hub predeterminado

```
<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/FullDefaultLayout">
        <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>
```

Ejemplo: Diseño de Inicio que incluye un vínculo de Microsoft Edge

Este ejemplo muestra un vínculo a un sitio web y un vínculo a un archivo .pdf. El icono secundario de Microsoft Edge usa un icono de 150 x 150 píxeles.

```
<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/FullDefaultLayout">
        <start:Group Name="" xmlns:start="http://schemas.microsoft.com/Start/2014/StartLayout">
    <start:Tile
              AppUserModelID="Microsoft.Office.PowerPoint_8wekyb3d8bbwe!Microsoft.pptim"
              Size="2x2"
              Row="0"
              Column="0"/>
          <start:Tile
              AppUserModelID="Microsoft.Office.Word_8wekyb3d8bbwe!Microsoft.Word"
              Size="2x2"
              Row="0"
              Column="2"/>
          <start:Tile
              AppUserModelID="Microsoft.Office.Excel_8wekyb3d8bbwe!Microsoft.Excel"
              Size="2x2"
              Row="0"
              Column="4"/>
          <start:DesktopApplicationTile
              DesktopApplicationID="MSEdge"
              Size="2x2"
              Row="2"
              Column="0"/>
    <start:Tile
              AppUserModelID="microsoft.microsoftskydrive_8wekyb3d8bbwe!App"
              Size="2x2"
             Row="2"
             Column="2"/>
  <start:SecondaryTile
            AppUserModelID="Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge"
           TileID="2678823080"
           DisplayName="Bing"
           Arguments="https://www.bing.com/"
           Square150x150LogoUri="ms-appx:///"
           Wide310x150LogoUri="ms-appx:///"
           ShowNameOnSquare150x150Logo="true"
           ShowNameOnWide310x150Logo="false"
           BackgroundColor="#ffe9e7e7"
           ForegroundText="dark"
           Size="2x2"
           Column="4"
           Row="2"  />
    <start:Tile
              AppUserModelID="Microsoft.Windows.Photos_8wekyb3d8bbwe!App"
              Size="2x2"
              Row="4"
              Column="0"/>
    <start:SecondaryTile
             AppUserModelID="Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge"
             TileID="6153963000"
             DisplayName="cstrtqbiology.pdf"
             Arguments="-contentTile -formatVersion 0x00000003 -pinnedTimeLow 0x45b7376e -pinnedTimeHigh
0x01d2356c -securityFlags 0x00000000 -tileType 0x00000000 -url 0x0000003a
https://www.ada.gov/regs2010/2010ADAStandards/Guidance_2010ADAStandards.pdf"
             Square150x150LogoUri="ms-appx:///Assets/MicrosoftEdgeSquare150x150.png"
             Wide310x150LogoUri="ms-appx:///"
             ShowNameOnSquare150x150Logo="true"
             ShowNameOnWide310x150Logo="false"
             BackgroundColor="#ff4e4248"
             Size="4x2"
             Row="4"
             Column="2"/>
        </start:Group>
      </defaultlayout:StartLayout>
```

```
    </StartLayoutCollection>
  </DefaultLayoutOverride>
</LayoutModificationTemplate>
```

> **NOTE**
>
> El valor predeterminado de es light; no es necesario incluirlo en el XML a menos que cambie el `ForegroundText` `ForegroundText` valor a oscuro.

Configurar y usar Microsoft Whiteboard

12/01/2022 • 3 minutes to read

La aplicación Pizarra de Microsoft incluye la funcionalidad de Surface Hubs y otros dispositivos con la aplicación Pizarra de Microsoft instalada para colaborar en tiempo real en el mismo tablero.

Requisitos previos

Para usar la colaboración en pizarras, complete las siguientes acciones:

- Agregue Whiteboard.ms, whiteboard.microsoft.com y wbd.ms a la lista de sitios permitidos.
- Puerto abierto: **HTTPS: 443** (normalmente configurado cuando ejecutas Por primera vez Surface Hub).

Requisitos de Office 365

- La colaboración en pizarra solo se admite en el entorno comercial de Office 365 y requiere Office 365 con Azure Active Directory basado en la nube (Azure AD).
- Solo puede ejecutar sesiones de colaboración entre usuarios pertenecientes al mismo inquilino de Office 365.
- Office 365 Germany u Office 365 operado por 21Vianet no admiten la colaboración en pizarras.

Colaboración con pizarras

Para iniciar una sesión de colaboración:

1. En la aplicación Pizarra, pulsa el botón **Iniciar sesión**.
2. Inicia sesión con el identificador de la organización.
3. Pulsa el botón **Invitar** situado junto a tu nombre, en la parte superior de la aplicación.
4. Escriba o escriba los nombres de los compañeros con los que desea colaborar.

En el otro dispositivo, como Surface Hub, cuando haya iniciado sesión, el tablero compartido aparecerá ahora en la galería de tableros.

Sugerencias de usuario

- Inicie sesión para obtener acceso a las pizarras. Mientras trabaja, los cambios se guardan automáticamente.
- Asigne un nombre a las pizarras para ayudar a organizar el contenido y encontrarlo rápidamente. Seleccione la opción ... para abrir el menú. Seleccione el **icono de** engranaje Opciones para obtener acceso a más herramientas y características de la pizarra.
- Usa **Ink para dar forma** para convertir el dibujo en formas reales como círculos, cuadrados y triángulos.
- Use **Ink to table** para convertir una cuadrícula dibujada en una tabla con filas y columnas.
- También puede cambiar el color de fondo y el diseño de sólido a cuadrícula o puntos. Elija el fondo y, a continuación, elija el color de la rueda que le rodea.
- Puede exportar una copia de la colaboración de pizarra por sí mismo a través del acceso Compartir y dejar la pizarra para que otros continúen trabajando.

Para obtener más información, consulta Usar la pizarra de Microsoft en un Surface Hub.

TIP

Si usa whiteboard y no puede iniciar sesión, puede colaborar uniéndose a una reunión de Teams o Skype Empresarial y, a continuación, compartir la pantalla. Una vez que haya terminado, pulse **Configuración Exportar**a > **correo electrónico** o guarde una copia del tablero. Si elige exportar a SVG, exporta gráficos vectoriales y proporciona una resolución mayor que PNG y se puede abrir en un explorador web.

Nuevas características en pizarra

La aplicación Pizarra de Microsoft, actualizada para Surface Hub el 1 de julio de 2019, incluye una gran cantidad de nuevas características, entre las que se incluyen:

- **Guardado automático:** los paneles se guardan en la nube automáticamente al iniciar sesión y se pueden encontrar en la galería de paneles. No hay ningún nombre de carpeta local ni directorio.
- **Colaboración extendida entre** dispositivos: puedes colaborar con nuevas aplicaciones para pc con Windows 10 e iOS, y una versión web para otros dispositivos.
- **Lienzo más enriquecido:** además de la tinta y las imágenes, la pizarra ahora incluye notas pegajosas, texto y GIF, con más objetos próximamente.
- **Inteligencia:** además de la tinta para la forma y la tabla, whiteboard ahora incluye la mejora de la tinta para mejorar la escritura a mano y la toma de lápiz para convertir imágenes en tinta.
- **Más opciones de color y fondo:** pizarra ahora incluye más colores de lápiz y opciones de grosor junto con colores de fondo y diseños adicionales.
- **Integración de Teams:** puede iniciar automáticamente pizarra desde una reunión de Teams y compartirla con los participantes.

Temas relacionados

- Windows 10 Creators Update para Surface Hub
- Documentación de soporte técnico de Microsoft Whiteboard
- Usar Microsoft Whiteboard en un Surface Hub

Finalizar una reunión de Surface Hub con Finalizar sesión

12/01/2022 • 4 minutes to read

Surface Hub es un dispositivo de colaboración que se ha diseñado para que lo usen distintos grupos de personas en espacios de reuniones. Al final de una reunión, los usuarios pueden presionar **Terminar la sesión** para limpiar los datos confidenciales y preparar el dispositivo para la próxima reunión. Surface Hub limpiará o restablecerá los siguientes estados:

- Aplicaciones
- Sistema operativo
- Interfaz de usuario

En este tema se explica qué restablece la opción **Terminar la sesión** para cada uno de estos estados.

Aplicaciones

Al iniciar aplicaciones en Surface Hub, estas se almacenan en la memoria y los datos se almacenan en el nivel de la aplicación. Estos datos están disponibles para todos los usuarios durante esa sesión (o reunión) hasta que se quitan o se sobrescriben. Cuando se selecciona **Terminar la sesión**, el estado de aplicación de Surface Hub se limpia mediante el cierre de aplicaciones, la eliminación del historial del navegador, el restablecimiento de las aplicaciones y la eliminación de los registros de Skype.

Cierre de aplicaciones

Surface Hub cierra todas las ventanas visibles, incluidas las aplicaciones Win32 y la Plataforma universal de Windows (UWP). La fase de cierre de aplicaciones usa la vista de multitarea para consultar las ventanas visibles. Las ventanas de Win32 que se cierran en un determinado período de tiempo se cierran mediante **TerminateProcess**.

Eliminación del historial del navegador

Surface Hub usa la función Eliminar historial del explorador (DBH) de Edge para borrar el historial de Edge y los datos almacenados en caché. Esto es similar a la forma en la que un usuario puede borrar el historial de su navegador manualmente, pero **Terminar la sesión** también garantiza que los estados de las aplicaciones se borran y los datos se eliminan antes de que empiece la siguiente sesión o reunión.

Restablecer las aplicaciones

Terminar la sesión restablece el estado de todas las aplicaciones instaladas en Surface Hub. El restablecimiento de una aplicación borra todas las tareas en segundo plano, los datos de las aplicaciones, las notificaciones y los cuadros de diálogo de consentimiento del usuario. Las aplicaciones vuelven a su estado de primera ejecución para las siguientes personas que usen Surface Hub.

Eliminación de los registros de Skype

Skype no almacena información de identificación personal en Surface Hub. La información se almacena en el servicio de Skype para cumplir con las pautas existentes de Skype Empresarial. La información de registro local de Skype son los únicos datos que se quitan cuando se selecciona **Terminar la sesión**. Esto incluye los registros de la plataforma unificada de cliente de comunicaciones (UCCP) y los registros multimedia.

Sistema operativo

El sistema operativo contiene una gran variedad de información sobre el estado de las sesiones que debe

borrarse después de cada reunión de Surface Hub.

Sistema de archivos

Los asistentes a la reunión tienen acceso a un conjunto limitado de directorios en Surface Hub. Cuando se selecciona **Terminar la sesión**, Surface Hub borra estos directorios:

- Música
- Vídeos
- Documentos
- Imágenes
- Descargas

Surface Hub, también borra estos directorios, dado que muchas aplicaciones a menudo escriben en ellos:

- Escritorio
- Favoritos
- Recientes
- Documentos públicos
- Música pública
- Vídeos públicos
- Descargas públicas

Credenciales

Las credenciales de usuario que se almacenan en **TokenBroker**, **PasswordVault** o el **Administrador de credenciales** se borran al pulsar **Terminar la sesión**.

Interfaz de usuario

Las opciones de configuración de la interfaz de usuario vuelven a sus valores predeterminados cuando se selecciona **Terminar la sesión**.

Elementos de la interfaz de usuario

- Restablecimiento de las acciones rápidas a su estado predeterminado
- Borrado de las notificaciones del sistema
- Restablecimiento de los niveles de volumen
- Restablecimiento del ancho de la barra lateral
- Restablecer el diseño del modo de tableta
- Cerrar la sesión del usuario en las reuniones y archivos de Office 365

Accesibilidad

Las características de accesibilidad y las aplicaciones se devuelven a la configuración predeterminada cuando se selecciona **Terminar la sesión**.

- Teclas de filtro
- Contraste alto
- Teclas especiales
- Teclas de alternancia
- Teclas del mouse
- Lupa
- Narrador

Portapapeles

El portapapeles se borra para eliminar los datos copiados en él durante la sesión.

Preguntas más frecuentes

¿Qué sucede si olvido pulsar Terminar la sesión al final de una reunión y otra persona usa Surface Hub más adelante?
Surface Hub solo limpia el contenido de las reuniones cuando los usuarios pulsan **Terminar la sesión**. Si abandonas la reunión sin pulsar **Terminar la sesión**, el dispositivo volverá a la pantalla de inicio de sesión transcurrido cierto tiempo. Desde la pantalla de inicio de sesión, los usuarios pueden reanudar la sesión anterior o iniciar una nueva. También puedes deshabilitar la posibilidad de reanudar la sesión si no se pulsa **Terminar la sesión**.

¿Los documentos se pueden recuperar?
La eliminación de archivos de la unidad de disco duro cuando se selecciona **Terminar la sesión** es igual que cualquier otra eliminación de archivos de una unidad de disco duro. Es posible que exista software de terceros que pueda recuperar datos de esta unidad de disco duro, pero la recuperación de archivos no es una característica compatible en Surface Hub. Para evitar la pérdida de datos, guarda siempre los datos que necesitas antes de salir de una reunión.

¿Las acciones de limpieza desde Terminar la sesión cumplen con el estándar de limpieza e higiene del Departamento de Defensa de los Estados Unidos DoD 5220.22-M?
No. Actualmente, las acciones de limpieza de **Terminar la sesión** no cumplen con este estándar.

Conectarse a otros dispositivos y mostrar su contenido con Surface Hub

12/01/2022 • 9 minutes to read

Puedes conectar otros dispositivos a tu Microsoft Surface Hub para mostrar su contenido. En este tema se describen el modo Invitado, el modo Equipo de reemplazo y la funcionalidad Salida de vídeo disponible a través de conexiones con cable, y también se indican los accesorios que se pueden conectar a Surface Hub mediante Bluetooth.

> **NOTE**
> Surface Hub la entrada de vídeo que selecciones hasta que se realiza una nueva conexión, se interrumpe la conexión existente o se cierra Conectar aplicación.

¿Qué método debo elegir?

Al conectar dispositivos y pantallas externas a Surface Hub, existen varias opciones. El método que uses dependerá del escenario y tus necesidades.

CUANDO QUIERAS:	USA ESTE MÉTODO:
Reflejar la pantalla de Surface Hub en otro dispositivo.	Salida de vídeo
Presentar la pantalla de otro dispositivo en la pantalla de Surface Hub e interactuar con el contenido del dispositivo y la experiencia integrada de Surface Hub.	Modo Invitado
Enciende Surface Hub desde un equipo externo con Windows 10 y apaga el equipo integrado de Surface Hub. Las cámaras, los micrófonos, los altavoces y otros periféricos se envían al equipo externo, además de las entradas de lápiz y táctiles.	Modo de equipo de reemplazo

Modo Invitado

El modo Invitado usa una conexión por cable para que los usuarios puedan mostrar el contenido de sus dispositivos en Surface Hub. Si el dispositivo de origen es un dispositivo Windows, dicho dispositivo también puede proporcionar touchback e inkback. El equipo interno de Surface Hub toma el audio y el vídeo del dispositivo conectado y los presenta en Surface Hub. Si Surface Hub encuentra una High-Bandwidth de protección de contenido digital (HDCP), el origen se mostrará como una imagen negra. Para mostrar tu contenido sin infringir los requisitos de HDCP, usa el teclado del lado derecho de Surface Hub para elegir directamente el origen externo.

> **NOTE**
> Cuando haya un origen HDCP conectado, usa el teclado lateral para cambiar las entradas de origen.

Puertos

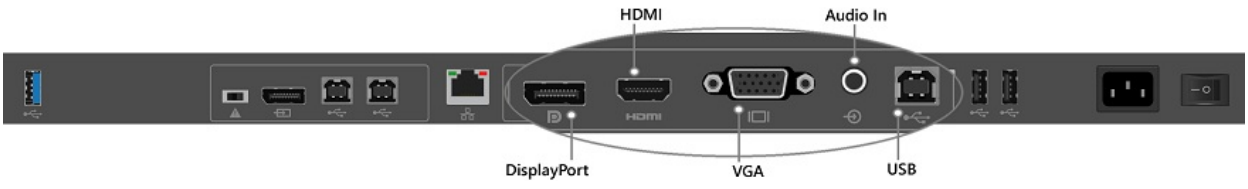
Usa estos puertos en Surface Hub para el modo Invitado.

INTERFAZ	TIPO	DESCRIPCIÓN	FUNCIONALIDADES
Puerto de pantalla 1.1a	Entrada de vídeo	Entrada de invitado 1	• Admite la visualización de esta entrada de invitado a la vez que la entrada de invitado 2 y la entrada de invitado 3 (una en alta resolución y dos en miniaturas). • Compatible con HDCP en el modo de omisión • Touchback habilitado
HDMI 1.4	Entrada de vídeo	Entrada de invitado 2	• Admite la visualización de esta entrada de invitado a la vez que la entrada de invitado 1 y la entrada de invitado 3 (una en alta resolución y dos en miniaturas). • Compatible con HDCP en el modo de omisión • Touchback habilitado

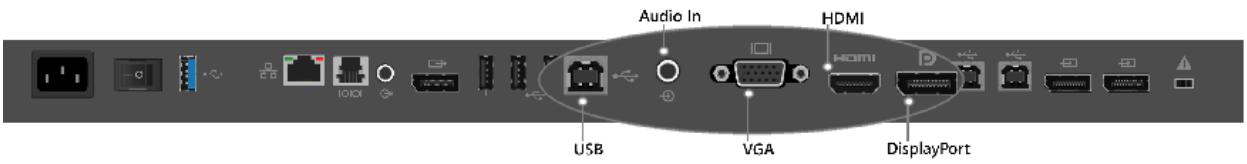
INTERFAZ	TIPO	DESCRIPCIÓN	FUNCIONALIDADES
VGA	Entrada de vídeo	Entrada de invitado 3	• Admite la visualización de esta entrada de invitado a la vez que la entrada de invitado 1 y la entrada de invitado 2 (una en alta resolución y dos en miniaturas). • Compatible con HDCP en el modo de omisión • Touchback habilitado
Conector de 3,5mm	Entrada de audio	Entrada de audio analógico	• Se consume en el equipo de Surface Hub, normalmente con la entrada de vídeo VGA.
USB 2.0, tipo B	Salida USB	Touchback	• Proporciona acceso los dispositivos de entrada HID (mouse, entrada táctil, teclado y el lápiz) de vuelta al equipo invitado.

Ubicaciones de los puertos

Estas son las conexiones de puerto usadas para el modo Invitado en Surface Hubs de 55" y de 84".



Conexiones de puerto cableadas en un Surface Hub de 55"



Conexiones de puerto cableadas en un Surface Hub de 84"

Enumeración de puertos

Cuando se conecta un Surface Hub a un equipo de invitado con el puerto USB de conexión cableada, se descubren y configuran varios dispositivos USB. Estos dispositivos periféricos se han creado para touchback e inkback. Los dispositivos periféricos pueden verse en el Administrador de dispositivos. El Administrador de dispositivos mostrará nombres duplicados para algunos dispositivos.

Dispositivos de interfaz humana (HID)

- Dispositivo de control del consumidor compatible con HID
- Lápiz compatible con HID
- Lápiz compatible con HID (elemento duplicado)
- Lápiz compatible con HID (elemento duplicado)
- Pantalla táctil compatible con HID
- Dispositivo de entrada USB
- Dispositivo de entrada USB (elemento duplicado)

Teclados

- Teclado PS/2 estándar

Mouse y otros dispositivos señaladores

- Mouse compatible con HID

Controladoras de bus serie universal

- Concentrador USB genérico
- Dispositivo compuesto USB

Conectividad de modo Invitado

La elección del cable de vídeo la determinará qué está disponible desde la entrada de origen. Surface Hub tiene 3 opciones de entrada de vídeo: DisplayPort, HDMI y VGA. Consulta el siguiente gráfico para conocer las resoluciones disponibles.

TIPO DE SEÑAL	RESOLUCIÓN	VELOCIDAD DE FOTOGRAMAS	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

El audio de origen lo proporcionan los cables de DisplayPort y HDMI. Si tienes que usar VGA, Surface Hub dispone de un puerto de entrada de audio que usa un conector de 3,5mm. Surface Hub también usa un cable USB que proporciona las capacidades de touchback e inkback desde Surface Hub a los dispositivos Windows10

compatibles. El cable USB puede usarse con cualquier entrada de vídeo que ya esté conectada con un cable.

Alguien que usa el modo Invitado para conectar un equipo usaría una de estas opciones:

DisplayPort: Cable DisplayPort y cable USB 2.0

HDMI: Cable HDMI y cable USB 2.0

VGA: Cable VGA, cable de audio de 3,5mm y cable USB 2.0

Si el equipo que usas para el modo Invitado no es compatible con touchback e inkback, el cable USB no será necesario.

Modo de equipo de reemplazo

En el modo Equipo de reemplazo, el equipo integrado de Surface Hub se apaga y se conecta un equipo externo a Surface Hub. Las conexiones con los puertos del equipo de reemplazo dan acceso a dispositivos periféricos clave de Surface Hub, lo que incluye la pantalla, el lápiz y las características táctiles. Esto significa que tu Surface Hub no tendrá el beneficio de la experiencia del Equipo de Windows, pero tendrás la flexibilidad que ofrecen el proporcionar y el administrar su propio equipo Windows.

Requisitos de software

Surface Hub puede ejecutarse en modo Equipo de reemplazo con las versiones de 64 bits de Windows10 Home, Windows10 Pro y Windows10 Enterprise. Puedes descargar el paquete de controladores de PC de reemplazo para Surface Hub desde el Centro de descarga de Microsoft. Te recomendamos que instales a estos controladores en cualquier equipo que vayas a usar como equipo de reemplazo.

Requisitos de hardware

Surface Hub es compatible con una gran variedad de hardware. Elige la confirmación del procesador y la memoria para el equipo de reemplazo, de forma que admita los programas que usarás. El hardware del equipo de reemplazo debe admitir las versiones de 64 bits de Windows10.

Tarjeta gráfica

En el modo Equipo de reemplazo, Surface Hub admite cualquier tarjeta gráfica que pueda producir una señal de DisplayPort. Mejorarás tu experiencia si usas una tarjeta gráfica que puede igualar la resolución y la frecuencia de actualización de Surface Hub. Por ejemplo, para obtener la mejor experiencia de equipo de reemplazo en Surface Hub, se recomienda una señal de vídeo de 120Hz.

Surface Hub 55": Para lograr la mejor experiencia, usa una tarjeta gráfica que admita una resolución de 1080p a 120Hz.

Surface Hub 84": Para lograr la mejor experiencia, usa una tarjeta gráfica que pueda generar 4 emisiones DisplayPort 1.2 para producir 2160p a 120Hz (3840 x 2160 con una actualización vertical de 120Hz). Hemos verificado que esto funciona con las tarjetas NVIDIA Quadro K2200, NVIDIA Quadro K4200, NVIDIA Quadro M6000, AMD FirePro W5100, AMD FirePro W7100 y AMD FirePro W9100. Estas no son las únicas tarjetas gráficas, ya que hay otras disponibles de otros proveedores.

Consulta directamente a los proveedores de tarjetas gráficas para obtener los controladores más recientes.

PROVEEDOR DE TARJETAS GRÁFICAS	PÁGINA DE DESCARGA DE CONTROLADORES
NVIDIA	http://nvidia.com/Download/index.aspx
AMD	http://support.amd.com/en-us/download

PROVEEDOR DE TARJETAS GRÁFICAS	PÁGINA DE DESCARGA DE CONTROLADORES
Intel	https://downloadcenter.intel.com/

Puertos

Puertos del equipo de reemplazo en Surface Hub 55".

DESCRIPCIÓN	TIPO	INTERFAZ	DETALLES
Vídeo del equipo	Entrada de vídeo	DP 1.2	• Visualización de pantalla completa de 1080p a 120 Hz, más audio • Compatible con HDCP
Periféricos internos	Salida USB	USB 2.0 tipo B	• Función táctil • Lápiz • Altavoces • Micrófono • Cámaras • Sensor NFC • Sensor de luz ambiental • Sensor de infrarrojos pasivo
Concentrador USB	Salida USB	USB 2.0 tipo B	• Puertos USB inferiores

Puertos del equipo de reemplazo en Surface Hub 84".

DESCRIPCIÓN	TIPO	INTERFAZ	DETALLES
Vídeo del equipo	Entrada de vídeo	DP 1.2 (2x)	• Visualización de pantalla completa de 2160p a 120 Hz, más audio • Compatible con HDCP
Periféricos internos	Salida USB	USB 2.0 tipo B	• Función táctil • Lápiz • Altavoces • Micrófono • Cámaras • Sensor NFC • Sensor de luz ambiental • Sensor de infrarrojos pasivo
Concentrador USB	Salida USB	USB 2.0 tipo B	• Puertos USB inferiores

Instrucciones de configuración para el equipo de reemplazo

Para usar el modo Equipo de reemplazo

1. Descarga e instala el paquete de controladores de PC de reemplazo para Surface Hub en el equipo de reemplazo.

   > **NOTE**
   > Te recomendamos que pongas el equipo de reemplazo en reposo o hibernación, ya que Surface Hub apagará la pantalla cuando no se use.

2. Apaga Surface Hub con el interruptor de alimentación situado junto al cable de alimentación.
3. Conecta los cables de los puertos del equipo de reemplazo de Surface Hub al equipo de reemplazo. Generalmente estos puertos se encuentra cubiertos por una tapa de plástico extraíble.

   Surface Hub 55": Conecta 1 cable DisplayPort y 2 cables USB.

   Surface Hub 84": Conecta 2 cables DisplayPort y 2 cables USB.

4. Cambia el conmutador de modo a **Equipo de reemplazo**. El conmutador de modo está junto a los puertos del equipo de reemplazo.
5. Enciende Surface Hub con el interruptor de alimentación situado junto al cable de alimentación.
6. Presiona el botón de alimentación en el lado derecho de Surface Hub.

Puedes cambiar Surface Hub para usar su PC interno.

Para volver a su PC interno

1. Apaga Surface Hub con el interruptor de alimentación situado junto al cable de alimentación.
2. Cambia el control de modo a PC interno. El conmutador de modo está junto a los puertos del equipo de reemplazo.
3. Enciende Surface Hub con el interruptor de alimentación situado junto al cable de alimentación.

Salida de vídeo

Surface Hub incluye un puerto de salida de vídeo para reflejar el contenido visual desde Surface Hub a otra pantalla.

Puertos

Puerto de salida de vídeo en Surface Hub 55"

Puerto de salida de vídeo en Surface Hub 84"

DESCRIPCIÓN	TIPO	INTERFAZ	FUNCIONALIDADES
Reflejo de salida de vídeo	Salida de vídeo	Salida de vídeo	• Admite la conexión a un monitor DisplayPort estándar (solo admite un vínculo x4 que muestre una resolución 1080p60 a 24bpp) • Admite el uso con monitores HDMI (compatibles con resoluciones de 1080p60) mediante un adaptador de DisplayPort a HDMI

Cables

Se ha demostrado que los dispositivos Surface Hub de 55" y 84" funcionan con cables DisplayPort certificados y con cables HDMI. Aunque algunos proveedores venden cables más largos que pueden funcionar con el Surface Hub, únicamente se garantiza el funcionamiento con dispositivos Surface Hub de aquellos cables certificados por laboratorios de pruebas. Por ejemplo, únicamente están certificados cables DisplayPort de hasta 3metros; sin embargo, muchos proveedores venden cables que tienen el triple de dicha longitud. Si es necesario un cable largo, recomendamos encarecidamente usar HDMI. HDMI posee muchas soluciones asequibles de cables de largo alcance, incluido el uso de repetidores. Casi todas las fuentes DisplayPort cambian automáticamente a señalización HDMI si se detecta un receptor HDMI.

Accesorios Bluetooth

Los accesorios siguientes pueden conectarse a Surface Hub mediante Bluetooth:

- Ratones
- Teclados
- Auriculares
- Altavoces

> **NOTE**
>
> Tras conectar unos auriculares o un altavoz Bluetooth, es posible que debas cambiar la configuración predeterminada de micrófono y altavoces.

Miracast sobre infraestructura

12/01/2022 • 3 minutes to read

En Windows 10, versión 1703, Microsoft ha ampliado la capacidad de enviar una emisión de Miracast a través de una red local, en lugar de a través de un vínculo directo inalámbrico. Esta funcionalidad se basa en el Protocolo de establecimiento de conexión de Miracast a través de infraestructura (MS-MICE).

Miracast a través de infraestructura ofrece una serie de ventajas:

- Windows detecta automáticamente cuándo se puede enviar la emisión de vídeo a través de esta ruta.
- Windows solo elige esta ruta si la conexión se realiza a través de Ethernet o de una red Wi-Fi segura.
- Los usuarios no tienen que cambiar la forma en que se conectan al receptor de Miracast. Usan la misma experiencia del usuario que en las conexiones de Miracast estándar.
- No es necesario realizar ningún cambio en los controladores inalámbricos existentes ni en el hardware del equipo.
- Funciona bien con el hardware inalámbrico más antiguo que no se haya optimizado para Miracast a través de Wi-Fi Direct.
- Aprovecha la conexión existente, lo que reduce el tiempo de conexión y ofrece una emisión muy estable.

Cómo funciona

Los usuarios intentan conectarse a un receptor Miracast a través de su Wi-Fi como lo hacían anteriormente. Cuando se llena la lista de receptores de Miracast, Windows 10 identificará el receptor que puede admitir una conexión a través de la infraestructura. Cuando el usuario selecciona un receptor de Miracast, Windows 10 intentará resolver el nombre de host del dispositivo a través de DNS estándar y de DNS multidifusión (mDNS). Si el nombre no se puede resolver a través de ninguno de estos métodos DNS, Windows 10 recurrirá a establecer la sesión de Miracast con la conexión de Wi-Fi Direct estándar.

> **NOTE**
> Para obtener más información sobre la secuencia de negociación de conexión, vea Miracast over Infrastructure Connection Establishment Protocol (MS-MICE)

Habilitar Miracast a través de la infraestructura

Si tienes un dispositivo Surface Hub u otro dispositivo con Windows 10 que se ha actualizado a Windows 10, versión 1703, tendrás automáticamente esta nueva característica. Para poder aprovecharla en el entorno, debes asegurarte de que se cumplan las siguientes condiciones en la implementación:

- Surface Hub o el dispositivo (PC o teléfono con Windows) debe ejecutar Windows 10, versión 1703.
- Puerto TCP abierto: **7250**.
- Surface Hub o un PC Windows se puede emplear como *receptor* de Miracast a través de la infraestructura. Un equipo o teléfono con Windows se puede emplear como *origen* de Miracast a través de la infraestructura.
  - Para que funcione como receptor de Miracast, Surface Hub o el dispositivo debe estar conectado a la red de empresa a través de Ethernet o de una conexión Wi-Fi segura (por ejemplo, con seguridad WPA2-PSK o WPA2-Enterprise). Si el Surface Hub o dispositivo está conectado a una conexión Wi-Fi abierta, Miracast sobre infraestructura se deshabilitará a sí mismo.
  - Para servir de origen de Miracast, el equipo o teléfono con Windows debe estar conectado a la misma red de empresa a través de Ethernet o de una conexión Wi-Fi segura.

- El nombre de host DNS (nombre de dispositivo) del Surface Hub o dispositivo debe resolverse a través de los servidores DNS. Puedes lograrlo permitiendo que Surface Hub se registre automáticamente a través de DNS dinámico, o crear manualmente un registro A o AAAA para el nombre de host de Surface Hub.
- Los equipos con Windows 10 deben estar conectados a la misma red de empresa a través de Ethernet o de una conexión Wi-Fi segura.

Es importante tener en cuenta que Miracast a través de la infraestructura no es un sustituto de Miracast estándar. Por el contrario, la funcionalidad es complementaria y ofrece ventajas a los usuarios que forman parte de la red de empresa. Los usuarios invitados en una determinada ubicación que no tengan acceso a la red de empresa seguirán conectándose mediante el método de conexión Wi-Fi Direct.

La opción de configuración **InBoxApps/WirelessProjection/PinRequired** en el proveedor de servicios de configuración (CSP) de SurfaceHub no es necesaria para Miracast a través de la infraestructura. Esto es porque Miracast a través de la infraestructura solo funciona si ambos dispositivos están conectados a la misma red de empresa. De este modo, se elimina de Miracast la restricción de seguridad que faltaba anteriormente. Te recomendamos que sigas usando esta opción de configuración (si la usabas anteriormente), ya que Miracast recurrirá a Miracast normal si la conexión a través de la infraestructura no funciona.

Preguntas más frecuentes

¿Por qué todavía necesito Wi-Fi usar Miracast sobre la infraestructura?
Las solicitudes de detección para identificar Miracast receptores solo se pueden producir a través del Wi-Fi adaptador. Una vez identificados los receptores, Windows 10 puede intentar la conexión a la red.

Habilitar la autenticación por cable 802.1X

12/01/2022 • 2 minutes to read

La actualización del 14 de noviembre de 2017 a Windows 10 (compilación 15063.726) habilitó directivas MDM de autenticación por cable 802.1x en Surface Hub dispositivos. La característica permite a las organizaciones aplicar la autenticación de red por cable estandarizada usando el protocolo de autenticación IEEE 802.1X. Esto ya estaba disponible para la autenticación inalámbrica mediante perfiles WLAN a través de MDM. En este tema se explica cómo configurar un Surface Hub para usarlo con la autenticación por cable.

La aplicación y la habilitación de la autenticación por cable 802.1X en Surface Hub se puede realizar a través de MDM definición de OMA-URI.

La configuración principal que se establecerá es la directiva **LanProfile**. Según el método de autenticación seleccionado, otras directivas pueden ser necesarias, ya sea la directiva **EapUserData** o a través de directivas de MDM para agregar certificados de usuario o equipo (como ClientCertificateInstall para certificados de usuario/dispositivo o RootCATrustedCertificates para certificados de dispositivo).

Elemento de directiva LanProfile

Para configurar Surface Hub para que use uno de los métodos de autenticación 802.1X admitidos, utilice el siguiente OMA-URI.

```
./Vendor/MSFT/SurfaceHub/Dot3/LanProfile
```

Este nodo de OMA-URI toma una cadena de texto de XML como parámetro. El XML proporcionado como parámetro debe cumplir el esquema de perfil de LAN con cable incluidos los elementos del esquema 802.1X.

En la mayoría de los casos, un usuario o administrador puede exportar el XML LanProfile desde un PC existente que ya esté configurado en la red para 802.1x con este comando NETSH.

```
netsh lan export profile folder=.
```

Al ejecutar este comando se mostrará el siguiente resultado y se colocará un archivo **Ethernet.xml** en el directorio actual.

```
Interface: Ethernet
Profile File Name: .\Ethernet.xml
1 profile(s) were exported successfully.
```

Elemento de directiva EapUserData

Si tu método de autenticación seleccionado requiere un nombre de usuario y una contraseña en lugar de un certificado, puedes usar el elemento **EapUserData** para especificar las credenciales para el dispositivo que se usará para autenticar en la red.

```
./Vendor/MSFT/SurfaceHub/Dot3/EapUserData
```

Este nodo de OMA-URI toma una cadena de texto de XML como parámetro. El XML proporcionado como

parámetro debe cumplir con el ejemplo de las propiedades de usuario de PEAP MS-CHAPv2. En el ejemplo, deberás reemplazar todas las instancias de *test* e *ias-domain* por tu información.

Agregar certificados

Si el método de autenticación seleccionado está basado en certificados, deberás crear un paquete de aprovisionamiento, usar MDMo importar un certificado de la configuración (**Configuración** > **Update and Security** > **Certificates**) para implementar dichos certificados en el dispositivo Surface Hub en el almacén de certificados adecuado. Al agregar certificados, cada PFX debe contener un certificado único (un PFX no puede tener varios certificados).

Uso de un sistema de control de la sala (Surface Hub)

12/01/2022 • 5 minutes to read

Los sistemas de control de la sala se pueden usar con tu Microsoft Surface Hub.

El uso de un sistema de control de la sala con el Surface Hub implica la conexión de hardware de control de la sala al Surface Hub, normalmente a través de un puerto serie RJ11 en la parte inferior del Surface Hub.

Configuración del terminal

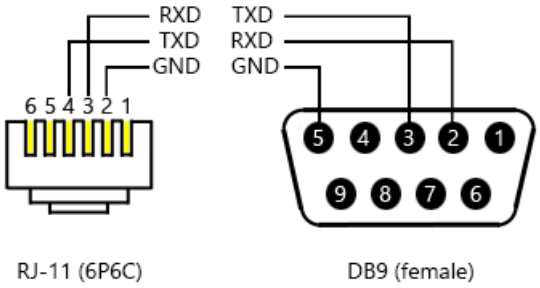
Para conectarte a un panel de control del sistema de control de la sala, no es necesario que configures ninguna terminal en el Surface Hub. Si quieres conectar un equipo o portátil al Surface Hub y enviar comandos de serie desde el Surface Hub, puedes usar un programa de emulador de terminal como Tera Term o PuTTY.

CONFIGURACIÓN	VALOR
Velocidad en baudios	115200
Bits de datos	4,8
Bits de parada	uno
Paridad	ninguno
Control de flujo	ninguno
Avance de línea	todos los retornos de carro

Diagrama del cableado

Puedes usar un conector RJ-11 (6P6C) estándar para conectar el puerto serie del Surface Hub con un sistema de control de la sala. Este es el método recomendado. También puedes usar un cable de 4 conductores RJ-11, pero no recomendamos este método.

Este diagrama muestra el patillaje correcto usado para un RJ-11 (6P6C) al cable DB9.



Conjuntos de comandos

Los sistemas de control de la sala usan escenarios comunes de sala de reuniones para los comandos. Los comandos se originan en el sistema de control de la sala y se comunican a través de una conexión serie a un

Surface Hub. Los comandos están basados en ASCII y el Surface Hub reconocerá cuando se produzcan cambios de estado.

Los siguientes modificadores de comandos están disponibles. Los comandos terminan en un carácter de nueva línea (/n). Las respuestas pueden presentarse en cualquier momento en respuesta a los cambios de estado no desencadenados directamente mediante un comando de puerto de administración.

MODIFICADOR	RESULTADO
+	Incrementar un valor
-	Disminuir un valor
=	Establecer un valor discreto
?	Consultas de un valor actual

Energía

El Surface Hub puede estar en uno de estos estados de energía.

ESTADO	ESTADO DE ENERGY STAR	DESCRIPCIÓN
,0	S5	Desactivado
uno	-	Encendido (indeterminado)
1	S3	Suspensión
4	S0	Ready

En el modo de PC de reemplazo, los estados de energía son solo Listo y Desactivado, y solo cambian la presentación. El puerto de administración no se puede usar para encender el equipo de reemplazo.

ESTADO	ESTADO DE ENERGY STAR	DESCRIPCIÓN
,0	S5	Apagado
4	S0	Listo

En el caso de un dispositivo de control, cualquier estado que no sea 5/Listo debería considerarse apagado. Cada comando de PowerOn da como resultado dos cambios y respuestas de estado.

COMANDO	CAMBIO DE ESTADO	RESPUESTA
Encendido	El dispositivo se activa (pantalla + PC). El servicio del equipo notifica a SMC que el equipo está listo.	Energía=0 Energía=5
Apagar	Transiciones del dispositivo al estado ambiental (PC encendido, atenuación de pantalla).	Energía=0

COMANDO	CAMBIO DE ESTADO	RESPUESTA
¿Energía?	SMC informa sobre el último estado de energía conocido.	Energía=<#>

Brillo

El nivel de brillo actual está en un intervalo de 0 a 100.

Los cambios en los niveles de brillo se pueden enviar mediante un sistema de control de la sala u otro sistema.

COMANDO	CAMBIO DE ESTADO	RESPUESTA
Brightness+	Controladora de administración del sistema (SMC) envía el comando de subir brillo. El servicio del equipo en el sistema de control de la sala notifica a SMC del nuevo nivel de brillo.	Brightness = 51
Brightness-	SMC envía el comando de bajar brillo. El servicio del equipo notifica a SMC del nuevo nivel de brillo.	Brightness = 50

Volumen

El nivel de volumen actual está en un intervalo de 0 a 100.

Los cambios en los niveles de volumen se pueden enviar mediante un sistema de control de la sala u otro sistema.

> **NOTE**
> El comando de volumen solo controlará el volumen para el modo incrustado o de equipo sustituto, no de orígenes invitados.

COMANDO	CAMBIO DE ESTADO	RESPUESTA (ACTIVA EN MODO DE EQUIPO SUSTITUTO)
Volume+	SMC envía el comando de subir volumen. El servicio del equipo notifica a SMC del nuevo nivel de volumen.	Volume = 51
Volume-	SMC envía el comando de bajar volumen. El servicio del equipo notifica a SMC del nuevo nivel de volumen.	Volume = 50

Silenciar audio

Se puede silenciar el audio.

COMANDO	CAMBIO DE ESTADO	RESPUESTA
AudioMute+	SMC envía el comando de silenciar audio. El servicio del equipo notifica a SMC que el audio está silenciado.	ninguno

Origen de vídeo

Se pueden usar varios orígenes de pantalla.

ESTADO	DESCRIPCIÓN
,0	Equipo incorporado
uno	DisplayPort
1	HDMI
2	VGA

Los cambios en el origen de pantalla los puede enviar un sistema de control de la sala u otro sistema.

COMANDO	CAMBIO DE ESTADO	RESPUESTA
Origen=#	SMC cambia al origen deseado. El servicio del equipo notifica a SMC que el origen de pantalla ha cambiado.	Origen=<#>
Source+	SMC pasa al siguiente origen de entrada activo. El servicio del equipo notifica a SMC del origen de entrada actual.	Origen=<#>
Origen-	SMC pasa al origen de entrada activo anterior. El servicio del equipo notifica a SMC del origen de entrada actual.	Origen=<#>
Source?	SMC consulta al servicio del equipo el origen de entrada activo. El servicio del equipo notifica a SMC del origen de entrada actual.	Origen=<#>

Errores

Los errores se devuelven según el formato de esta tabla.

ERROR	NOTAS
Error: Comando desconocido '<input>'.	La instrucción contiene un comando inicial desconocido. Por ejemplo, "VOL+" no sería válido y se devolvería " Error: Comando desconocido 'VOL'".
Error: Operador desconocido '<input>'.	La instrucción contiene un operador desconocido. Por ejemplo, "Volume!" no sería válido y se devolvería " Error: Operador desconocido '!'".
Error: Parámetro desconocido '<input>'.	La instrucción contiene un parámetro desconocido. Por ejemplo, "Volume=abc" no sería válido y se devolvería " Error: Parámetro desconocido 'abc'".
Error: Comando no disponible cuando está desactivado '<input>'.	Cuando el Surface Hub está desactivado, los comandos que no sean Power devuelven este error. Por ejemplo, "Volume+" no sería válido y se devolvería " Error: Comando no disponible cuando está desactivado 'Volume'".

Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Iniciar sesión en Surface Hub con Microsoft Authenticator

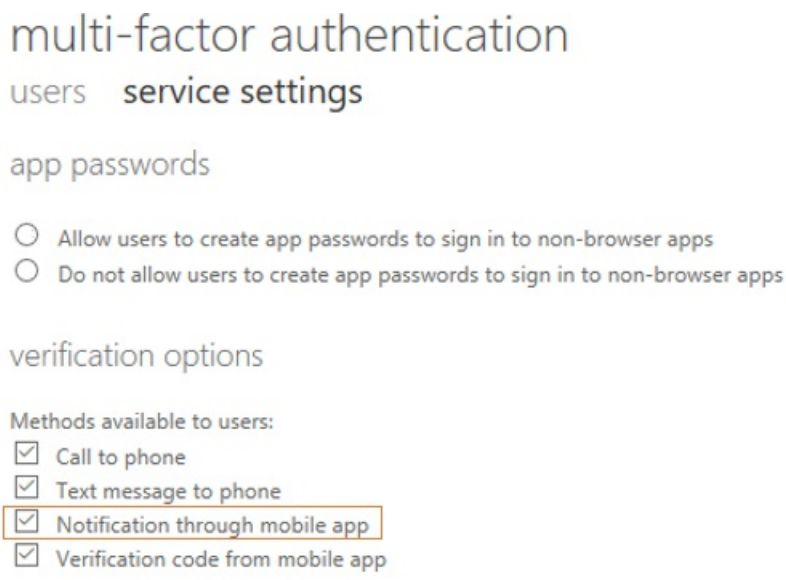
12/01/2022 • 2 minutes to read

Las personas de tu organización pueden iniciar sesión en un dispositivo Surface Hub sin una contraseña con la aplicación Microsoft Authenticator, disponible en Android e iOS.

Requisitos previos de la organización

Para permitir que las personas de tu organización inicien sesión en Surface Hub con sus teléfonos y otros dispositivos en lugar de una contraseña, tendrás que asegúrate de que la organización cumple estos requisitos previos:

- La organización debe tener un entorno híbrido o solo en la nube, respaldada por la solución Azure Active Directory (Azure AD). Para más información, consulta ¿Qué es Azure Active Directory?.
- Asegúrate de tener como mínimo una suscripción a Office 365 E3.
- Configurar la autenticación multifactor. Asegúrate de que la opción **Notificación a través de aplicación móvil** está seleccionada.



- Habilitar el hospedaje de contenido en servicios de Azure AD como Office, SharePoint, etc.
- Surface Hub debe ejecutar Windows 10, versión 1703 o posterior.
- Surface Hub está configurado con una cuenta local o unida a un dominio.

Requisitos previos individuales

- Un teléfono Android que ejecuta 6.0 o versión posterior, o un iPhone o iPad que ejecuta iOS9 o versión posterior
- La versión más reciente de la aplicación Microsoft Authenticator de la tienda de aplicaciones adecuada

> **NOTE**
>
> En iOS, la versión de la aplicación debe ser 5.4.0 o superior.
>
> La aplicación Microsoft Authenticator en teléfonos con un sistema operativo Windows no pueden usarse para iniciar sesión en Surface Hub.

- El código de acceso o pantalla de bloqueo están habilitados en el dispositivo

Cómo configurar la aplicación Microsoft Authenticator

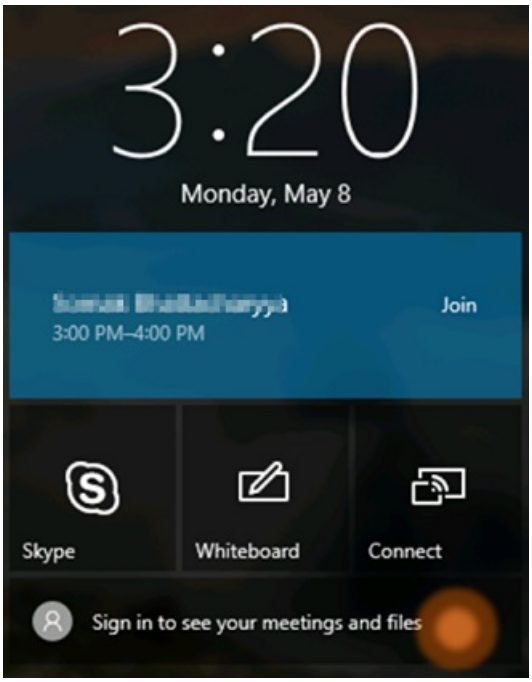
> **NOTE**
>
> Si el Portal de empresa está instalado en tu dispositivo Android, desinstálalo antes de configurar Microsoft Authenticator. Después de configurar la aplicación, puedes reinstalar Portal de empresa.
>
> Si ya has configurado Microsoft Authenticator en tu teléfono y has registrado tu dispositivos, ve a las instrucciones de inicio de sesión.

1. Agrega tu cuenta profesional o educativa a Microsoft Authenticator para la autenticación multifactor. Necesitarás un código QR proporcionado por el departamento de TI. Para obtener ayuda, consulta Introducción a la aplicación Microsoft Authenticator.
2. Ve a **Configuración** y registrar tu dispositivo.
3. Vuelve a la página de cuentas y elige **Habilitar el inicio de sesión en el teléfono** en el menú desplegable Cuenta.

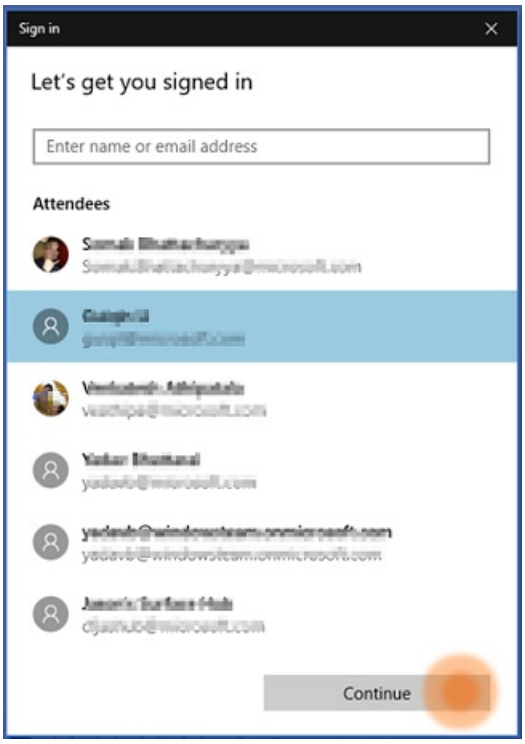
Cómo iniciar sesión en Surface Hub durante una reunión

1. Después de configurar una reunión, ve a Surface Hub y selecciona **Inicia sesión para ver las reuniones y los archivos**.

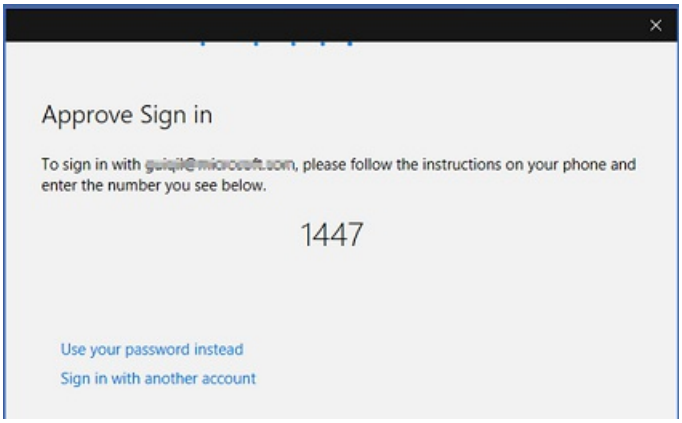
   > **NOTE**
   >
   > Si no está seguro cómo programar una reunión en Surface Hub, consulta Programar un Surface Hub.

2. Verás una lista de las personas invitadas a la reunión. Selecciónate a ti mismo (o selecciona la persona que quiere iniciar sesión, asegurándote de que esta persona haya realizado los pasos para configurar su dispositivo antes de la reunión) y luego selecciona **Continuar**.



Verás un código en el dispositivo Surface Hub.



3. Para aprobar el inicio de sesión, abre la aplicación Authenticator, escribe el código de cuatro dígitos que se muestra en Surface Hub y selecciona **Aprobar**. Se te pedirá que especifiques el PIN o que uses tu huella digital para completar el inicio de sesión.

Ahora puedes acceder a todos los archivos a través de la aplicación OneDrive.

Guardar la clave de BitLocker (Surface Hub)

12/01/2022 • 2 minutes to read

Cada Microsoft Surface Hub se configura automáticamente con el software de cifrado de unidad de BitLocker. Microsoft recomienda encarecidamente que te asegures de hacer una copia de seguridad de las claves de recuperación de BitLocker.

Hay varias maneras de administrar la clave de BitLocker en Surface Hub.

1. Si uniste Surface Hub a un dominio, el dispositivo realizará una copia de seguridad de la clave del dominio y la almacenará en el objeto del equipo.

   Si no encuentras la clave de BitLocker después de unir el dispositivo a un dominio, es probable que tu esquema de Active Directory no admita la copia de seguridad de la clave de BitLocker. Si no quieres cambiar el esquema, puedes guardar la clave de BitLocker yendo a Configuración y siguiendo el procedimiento para usar una cuenta de administrador local, lo que se detallará más adelante en esta lista.

2. Si has unido Surface Hub a Azure Active Directory (Azure AD), la clave de BitLocker se almacenará en la cuenta usada para unir el dispositivo.

3. Si está usando una cuenta de administrador local para administrar el dispositivo, puede guardarla en la aplicación **configuración** y navegar para **Actualizar &** la > **recuperación**de seguridad. Inserta una unidad USB y selecciona la opción para guardar la clave de BitLocker. La clave se guardará en un archivo de texto en la unidad USB.

Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Autenticación moderna en Surface Hub

12/01/2022 • 2 minutes to read

La actualización de Windows 10 Team 2020 agrega compatibilidad con la autenticación moderna de la cuenta del dispositivo Hub en algunos escenarios. Una vez instalada la actualización de 2020, puede migrar desde la autenticación básica heredada para usar las mejoras de seguridad más recientes si la cuenta del dispositivo se autentica a través de Azure Active Directory y el buzón de la cuenta está hospedado en Exchange Online. Con la actualización de 2020, Surface Hub admite protocolos de Exchange Web Services (EWS) y autenticación basada en la Biblioteca de autenticación de Active Directory (ADAL) al sincronizar la cuenta del dispositivo con Exchange Online.

Para las nuevas cuentas basadas en la nube, Surface Hub usa automáticamente la autenticación moderna para conectarse a Exchange Online sin necesidad de configuración adicional más allá de simplemente agregar la cuenta de dispositivo a Surface Hub con el formato alias@contoso.com. No use el formato heredado: Contoso\alias, que no es compatible con la autenticación moderna. Para obtener más información, consulta crear y probar una cuenta de dispositivo.

> **NOTE**
> La autenticación moderna no es compatible con las cuentas locales de Surface Hub. Las cuentas solo deben usar Azure AD para la autenticación.

Configurar el inicio de sesión sin contraseña en Surface Hub

12/01/2022 • 3 minutes to read

El inicio de sesión sin contraseña simplifica el acceso a sus aplicaciones, reuniones y archivos. Surface Hub permite iniciar sesión con la aplicación Microsoft Authenticator y las claves de seguridad fido2 proporcionadas por la organización.

Importante: Este contenido está destinado a los usuarios. Para usar el inicio de sesión sin contraseña, el administrador de TI debe habilitar la autenticación sin contraseña para su organización. Para más información, consulta lo siguiente:

- Habilitar el inicio de sesión de teléfono sin contraseña
- Habilitar el inicio de sesión con clave de seguridad sin contraseña

Configurar el inicio de sesión con Microsoft Authenticator aplicación

Nota: A partir de Windows 10 Team actualización de 2020, los usuarios pueden usar sus alias de correo electrónico preferidos en Azure AD, así como su nombre principal de usuario (UPN), para iniciar sesión con Microsoft Authenticator. Por ejemplo, un usuario puede usar su alias preferido (John.Doe@contoso.com) o su UPN (jdoe@contoso.com) para iniciar sesión.

La Microsoft Authenticator te ayuda a iniciar sesión en Surface Hub usar el dispositivo móvil. Para configurar el inicio de sesión con Microsoft Authenticator:

1. En el dispositivo móvil, descarga la Microsoft Authenticator aplicación.
   - Google Android: en tu dispositivo Android, ve a Google Play para descargar e instalar la Microsoft Authenticator aplicación.
   - Apple iOS: en tu dispositivo Apple iOS, ve a la App Store para descargar e instalar la Microsoft Authenticator aplicación.
2. En el equipo, configura la aplicación Microsoft Authenticator desde la página Información de seguridad de tu cuenta laboral o educativa.
3. Desde la Microsoft Authenticator en tu dispositivo móvil, activa y usa el inicio de sesión del teléfono para tu cuenta laboral o educativa.

Configurar el inicio de sesión con claves de seguridad FIDO2

> **NOTE**
> El inicio de sesión sin contraseña Surface Hub con claves de seguridad FIDO2 requiere la actualización Windows 10 Team 2020.

> **IMPORTANT**
> Surface Hub solo admite claves de seguridad USB.

También puede iniciar sesión en Surface Hub con una clave de seguridad FIDO2 proporcionada por su organización.

Para configurar el inicio de sesión con una clave de seguridad:

1. En el equipo, vaya a la página e inicie sesión en su cuenta laboral https://myprofile.microsoft.com/ o educativa.
2. Selecciona **Información de seguridad** en el panel **** de navegación izquierdo o en el vínculo del bloque Información de seguridad y, a continuación, selecciona **Agregar** método en la página **Información de** seguridad.
3. En la **página Agregar un método,** seleccione Clave **de seguridad** de la lista desplegable y, a continuación, **seleccione Agregar**.
4. En la **página Clave de** seguridad, elija Dispositivo **USB**.
5. Tenga la clave de seguridad lista y seleccione **Siguiente**.
6. En el cuadro de diálogo que aparece, siga las instrucciones para insertar la clave de seguridad, crear o escribir un PIN y realizar el gesto necesario (ya sea biométrico o táctil).
7. En la **página Clave de** seguridad, asigne un nombre a la clave de seguridad y, a continuación, seleccione **Siguiente**.
8. Seleccione **Listo** para completar el proceso.

Inicie sesión en Surface Hub

Una vez que hayas configurado el inicio de sesión sin contraseña, puedes usarlo para facilitar el acceso a tus aplicaciones, reuniones y archivos en el Surface Hub:

- Únase rápidamente a sus reuniones y abra archivos Microsoft 365 recientes. Para obtener más información, vea **Iniciar sesión para ver sus reuniones y archivos.**
- Inicie sesión rápidamente en aplicaciones de Microsoft como Whiteboard, PowerPoint, Word, Excel, OneDrive y Power BI.
- Inicie sesión rápidamente en el nuevo Microsoft Edge para acceder a sus preferencias de navegación y favoritos. Para obtener más información, vea Install and configure the new Microsoft Edge.
- Una vez que hayas iniciado sesión Surface Hub, puedes usar otras aplicaciones sin tener que volver a iniciar sesión hasta que **selecciones Finalizar sesión**. Al seleccionar **Finalizar sesión,** se eliminan las credenciales, los archivos y los datos personales del dispositivo. Para obtener más información, vea End session.

Obtén más información

- Opciones de autenticación sin contraseña para Azure Active Directory
- Inicio de sesión sin contraseña con la Microsoft Authenticator aplicación
- Inicio de sesión sin contraseña con claves de seguridad FIDO2

Cómo gestiona Surface Hub los problemas de seguridad de Wi-Fi Direct

12/01/2022 • 13 minutes to read

Microsoft Surface Hub es un dispositivo de productividad todo en uno que permite a los equipos realizar una mejor lluvia de ideas, colaborar y compartir ideas. Surface Hub depende de Miracast para la proyección inalámbrica a través de Wi-Fi Direct.

En este artículo se describen las vulnerabilidades de seguridad de Wi-Fi Direct, cómo afronta Surface Hub esos riesgos y cómo los administradores pueden configurar Surface hub para obtener el mayor nivel de seguridad. Esta información ayudará a los clientes que tienen requisitos de alta seguridad a proteger sus redes conectadas en el Hub y los datos en tránsito.

Las audiencias previstas para este artículo son administradores de ti y de redes que desean implementar Surface Hub en su entorno corporativo con una configuración de seguridad óptima.

Introducción

La seguridad de Surface Hub depende ampliamente de Wi-Fi Direct/Miracast y de los estándares asociados de 802,11, Wi-Fi Protected Access (WPA2) y de configuración protegida inalámbrica (WPS). Dado que el dispositivo solo es compatible con WPS (a diferencia de la clave previamente compartida de WPA2 o WPA2 Enterprise), los problemas que se suelen asociar con el cifrado de 802,11 se simplifican.

Surface Hub funciona de su equivalente con el campo de los receptores Miracast. Por lo tanto, es vulnerable a un conjunto similar de exploits que todos los dispositivos de red inalámbrica basados en WPS. Pero la implementación de Surface Hub de WPS tiene precauciones adicionales integradas. Además, su arquitectura interna ayuda a evitar que un atacante que ha puesto en peligro la capa Wi-Fi Direct o Miracast pase la interfaz de red a otras superficies de ataque y redes empresariales conectadas.

Wi-Fi Direct en segundo plano

Miracast forma parte del estándar de visualización de Wi-Fi, que es compatible con el protocolo Wi-Fi Direct. Estos estándares son compatibles con dispositivos móviles modernos para colaboración y uso compartido de pantalla.

Wi-Fi Direct o Wi-Fi "de par a par" (P2P) es un estándar de la Alianza Wi-Fi para redes "ad-hoc". Los dispositivos compatibles pueden comunicarse directamente y crear grupos de redes sin un punto de acceso o conexión a Internet convencional.

WPA2 proporciona seguridad para Wi-Fi Direct en el estándar WPS. El mecanismo de autenticación para dispositivos puede ser un PIN numérico (código PIN de WPS), un botón de inserción físico o virtual (WPS-PBC) o un mensaje fuera de banda, como una comunicación Near Field (WPS-OOO). Surface Hub admite el método de ANCLAr y el método pulsador, que es el predeterminado.

En Wi-Fi Direct, los grupos se crean como uno de los siguientes tipos:

- *Persistente*, en el que puede realizarse la reconexión automática mediante material de clave almacenado
- *Temporal*, en el que los dispositivos no pueden volver a autenticarse sin la acción del usuario

Los grupos de Wi-Fi Direct determinan el propietario de un *Grupo* (ir) a través de un protocolo de negociación, que imita la funcionalidad "estación" o "punto de acceso" para el grupo de Wi-Fi Direct establecido. Wi-Fi Direct

GO proporciona autenticación (a través de un "registrador interno") y facilita la transmisión de conexiones de red. Para Surface Hub, la negociación de este GO no se produce. La red solo funciona en modo "autónomo" y Surface Hub siempre es el propietario del grupo. Por último, Surface Hub no se une a otras redes Wi-Fi Direct como cliente.

Cómo afronta Surface Hub las vulnerabilidades de Wi-Fi Direct

Vulnerabilidades y ataques en las invitaciones directas, la difusión y el proceso de detección de Wi-Fi: Los ataques de Wi-Fi Direct/Miracast pueden dirigirse a debilidades en el establecimiento de grupos, detección de elementos de mismo nivel, difusión de dispositivo o procesos de invitación.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
El proceso de descubrimiento puede permanecer activo durante un período de tiempo prolongado, lo que puede permitir que se establezcan invitaciones y conexiones sin la aprobación del propietario del dispositivo.	Surface Hub solo funciona como propietario del grupo, que no realiza los procesos de negociación o descubrimiento de clientes. Puede desactivar completamente la proyección inalámbrica para desactivar la difusión.
Invitación y descubrimiento a través de PBC permite que un atacante no autenticado realice repetidos intentos de conexión o se acepten conexiones no autenticadas de forma automática.	Al requerir la seguridad del PIN de WPS, los administradores pueden reducir el potencial de conexiones no autorizadas o "bombas de invitación" en las que las invitaciones se envían repetidamente hasta que un usuario acepta por error.

Botón de comando de configuración de Wi-Fi Protected Setup (WPS) Connect (PBC) vs: Se han demostrado puntos débiles públicos en el diseño y la implementación de métodos de WPS-PIN. WPS-PBC tiene otras vulnerabilidades que podrían permitir ataques activos contra un protocolo diseñado para un uso único.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
WPS-PBC es vulnerable a atacantes activos. La especificación de WPS dice: "el método PBC tiene cero bits de entropía y solo protege contra ataques de escucha pasiva. PBC protege contra los ataques de interceptación y toma medidas para evitar que un dispositivo se una a una red que no seleccionó el propietario del dispositivo. Sin embargo, la ausencia de autenticación significa que PBC no protege contra un ataque activo. " Los atacantes pueden usar una interconexión inalámbrica selectiva o cualquier otra técnica de denegación de servicio para desencadenar una conexión o un conexión Wi-Fi Direct o no deseada. Además, un atacante activo que simplemente tiene la proximidad física puede destruir varias veces cualquier grupo de Wi-Fi Direct e intentar el ataque hasta que se complete.	Habilitar la seguridad de PIN de WPS en la configuración de Surface Hub. La especificación WPS de Wi-Fi dice: "el método PBC solo se debe usar si no hay registrador con capacidad para PIN y el usuario de WLAN está dispuesto a aceptar los riesgos asociados con PBC".
Las implementaciones de PIN de WPS pueden estar sujetas a ataques de fuerza bruta que se destinan a una vulnerabilidad en el estándar de WPS. El diseño de la verificación de PATILLAs dividida condujo varias vulnerabilidades de implementación durante los últimos años en una variedad de fabricantes de hardware de Wi-Fi. En 2011, los investigadores Martín Viehböck y Craig Heffner publicaron información sobre esta vulnerabilidad y herramientas como "Reaver" como prueba de concepto.	La implementación de Microsoft de WPS en Surface Hub cambia el PIN cada 30 segundos. Para descifrar el PIN, un atacante debe completar todo el exploit en menos de 30 segundos. Dado el estado actual de las herramientas y la investigación en esta área, es poco probable que un ataque de craqueo a PIN de fuerza bruta a través de WPS tenga éxito.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
WPS-PIN se puede adivinar mediante un ataque sin conexión debido a una clave inicial débil (E-S1, E S2) entropía. En 2014, Dominique Bongard describía un ataque de "polvo Pixie" en el que la aleatoriedad inicial del generador de números pseudoaleatorios (PRNG) en el dispositivo inalámbrico permitía un ataque de fuerza bruta sin conexión.	La implementación de Microsoft de WPS en Surface Hub no es susceptible a este ataque de la fuerza bruta sin conexión. El PIN de WPS es aleatorio para cada conexión.

Exposición no deseada de servicios de red: Los daemons de red pensados para los servicios de Ethernet o WLAN pueden exponerse accidentalmente debido a un error de configuración (como el enlace a interfaces "todas"/0.0.0.0). Otras causas posibles son que el firewall del dispositivo esté mal configurado o que falten reglas de Firewall.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Un error de configuración enlaza un servicio de red no autenticado o vulnerable a interfaces "all", incluida la interfaz de Wi-Fi Direct. Esto puede exponer servicios que no deberían ser accesibles para clientes de Wi-Fi Direct, que pueden autenticarse de manera débil o automática.	En Surface Hub, las reglas de Firewall predeterminadas solo permiten los puertos de red TCP y UDP requeridos y deniegan de forma predeterminada todas las conexiones entrantes. Habilite el modo de PIN de WPS para configurar la autenticación robusta.

Puentes de Wi-Fi Direct y otras redes cableadas o inalámbricas: El puente de red entre redes WLAN o Ethernet es una violación de la especificación Wi-Fi Direct. Un puente o una configuración no recomendable puede reducir o quitar de forma eficaz los controles de acceso inalámbrico para la red corporativa interna.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Los dispositivos de Wi-Fi Direct podrían permitir acceso no autenticado o deficiente para las conexiones de red conectadas. Esto podría permitir que las redes Wi-Fi Direct enruten el tráfico a una LAN Ethernet interna u otra infraestructura o a redes WLAN de la empresa infringiendo los protocolos de seguridad de TI existentes.	Surface Hub no se puede configurar para enlazar interfaces inalámbricas o permitir el enrutamiento entre redes dispares. Las reglas de firewall predeterminadas agregan una defensa más profunda para este tipo de conexiones de enrutamiento o puente.

El uso del modo Wi-Fi Direct "heredado": La exposición a redes o dispositivos no deseados puede producirse cuando opera en modo "heredado". Si no está habilitado el PIN de WPS, se podrían producir conexiones no intencionadas o suplantación de identidades del dispositivo.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Al ser compatible con los clientes de infraestructura 802.11 y Wi-Fi Direct, el sistema funciona en un modo de compatibilidad "heredado". Esto puede exponer la fase de configuración de la conexión de forma indefinida, lo que permite que los grupos se unan o los dispositivos invitados a conectarse correctamente después de finalizar la fase de configuración previstas.	Surface Hub no es compatible con clientes heredados de Wi-Fi Direct. Solo se pueden realizar conexiones de Wi-Fi Direct a Surface Hub, incluso cuando el modo PIN de WPS está habilitado.

Negociación de Wi-Fi Direct go durante la configuración de la conexión: El propietario del grupo en Wi-Fi Direct es análogo al "punto de acceso" en una red inalámbrica de 802,11 convencionales. Un dispositivo malintencionado puede sortear la negociación.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Si se establecen dinámicamente grupos o se puede hacer que el dispositivo Wi-Fi Direct se unan a grupos nuevos, la negociación de propietarios del grupo puede hacerse con un dispositivo malintencionado que siempre especifica el valor máximo de 15 como propietario del grupo. (Pero se produce un error en la conexión si el dispositivo está configurado para ser siempre un propietario del grupo).	Surface Hub aprovecha el modo autónomo "Wi-Fi Direct", que omite la fase de negociación GO de configuración de conexión. Y Surface Hub siempre es el propietario del grupo.

Desautenticación de Wi-Fi inesperada o malintencionada: La desautenticación Wi-Fi es un ataque antiguo en el que un atacante local puede acelerar la pérdida de información en el proceso de configuración de la conexión, desencadenar nuevos protocolos de enlace de cuatro vías, dirigirse a una versión de Wi-Fi Direct-PBC para ataques activos o crear ataques de denegación de servicio.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Los atacantes no autenticados pueden enviar paquetes de deautenticación para hacer que la estación se vuelva a autenticar y rastrear el protocolo de enlace resultante. Pueden intentarse ataque criptográfico o de fuerza bruta en el protocolo de enlace resultante. La mitigación de estos ataques incluye la aplicación de directivas de longitud y complejidad para las claves previamente compartidas, la configuración del punto de acceso (si procede) para detectar niveles malintencionados de paquetes de desautenticación y el uso de WPS para generar automáticamente claves seguras. En el modo PBC, el usuario interactúa con un botón físico o virtual para permitir una asociación de dispositivo arbitraria. Este proceso solo debe realizarse durante la configuración, en un breve lapso de tiempo. Después de insertar el botón automáticamente, el dispositivo aceptará cualquier estación que se asocie a un valor de PIN canónico (todos los ceros). La desautenticación puede forzar un proceso de instalación repetido.	Surface Hub usa WPS en modo PIN o PBC. No se permite ninguna configuración de PSK. Este método ayuda a exigir la generación de claves sólidas. Lo mejor es habilitar la seguridad de PIN de WPS para Surface Hub.
Además de los ataques de denegación de servicio, los paquetes de desautenticación se pueden usar para desencadenar una reconexión que vuelva a abrir la ventana de oportunidad de ataques activos contra WPS-PBC.	Habilitar la seguridad de PIN de WPS en la configuración de Surface Hub.

Revelación de información inalámbrica básica: Las redes inalámbricas, 802,11 o de otro modo, son inherentes al riesgo de revelación de información. Aunque esta información es principalmente metadatos de conexión o dispositivo, este problema sigue siendo un riesgo conocido para cualquier administrador de red de 802,11. Wi-Fi Direct con autenticación de dispositivos a través de PIN de WPS revela eficazmente la misma información como una red PSK o Enterprise 802.11

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Durante la difusión, la configuración de la conexión o incluso el funcionamiento normal de las conexiones ya cifradas, la información básica sobre los dispositivos y los tamaños de los paquetes es transmitida de manera inalámbrica. En un nivel básico, un atacante local que se encuentra dentro del rango inalámbrico puede examinar los elementos de información de 802,11 pertinentes para determinar los nombres de los dispositivos inalámbricos, las direcciones MAC de los equipos de comunicación y posiblemente otros detalles, como la versión de la pila inalámbrica, los tamaños de paquete o las opciones del punto de acceso configurado o el propietario del grupo.	La red Wi-Fi Direct que usa Surface Hub no puede protegerse aún más de las pérdidas de metadatos, como las de 802,11 Enterprise o PSK Wireless. La seguridad física y la eliminación de las amenazas potenciales de la proximidad inalámbrica pueden ayudar a reducir las fugas potenciales en información.

Ataques inalámbricos de gemelas o de suplantación: La suplantación de nombre inalámbrico es un ataque sencillo y muy conocido que puede usar un atacante local para atraer a usuarios insospechados o malintencionados para que se conecten.

VULNERABILIDAD DE WI-FI DIRECT	MITIGACIÓN DEL SURFACE HUB
Al imitar o clonar el nombre inalámbrico o el "SSID" de la red de destino, un atacante puede engañar al usuario para que se conecte a una red falsa y malintencionada. Al permitir la combinación automática de Miracast sin autenticar, un atacante podría capturar los materiales de visualización previstos o lanzar ataques de red en el dispositivo de conexión.	Aunque no existen protecciones específicas contra la Unión a un Surface Hub imitado, esta vulnerabilidad se ha mitigado parcialmente de dos maneras. En primer lugar, cualquier potencial ataque debe producirse físicamente dentro del alcance Wi-Fi. En segundo lugar, este ataque solo es posible durante la primera conexión. Las conexiones posteriores usan un grupo de Wi-Fi Direct persistente y Windows recordará y establecerá la prioridad de esta conexión anterior durante el uso del concentrador. (Nota: no se consideró la suplantación de la dirección MAC, el canal Wi-Fi y el SSID al mismo tiempo para este informe y esto puede dar lugar a un comportamiento de Wi-Fi incoherente). En general, este punto débil es un problema fundamental para cualquier red inalámbrica de 802,11 que carezca de protocolos de WPA2 empresarial como EAP-TLS o EAP-PWD, que no es compatible con Wi-Fi Direct.

Directrices de refuerzo de Surface Hub

Surface Hub está diseñado para facilitar la colaboración y permitir que los usuarios puedan iniciar o unirse a reuniones de una manera rápida y eficaz. La configuración predeterminada de Wi-Fi Direct para Surface Hub está optimizada para este escenario.

Para la seguridad de interfaz inalámbrica adicional, los usuarios de Surface Hub deben habilitar la configuración de seguridad de WPS-PIN. Esta opción deshabilita el modo WPS-PBC y ofrece autenticación de cliente. Proporciona el nivel de protección más potente evitando la conexión no autorizada a Surface Hub.

Si aún tienes dudas sobre la autenticación y la autorización de Surface Hub, te recomendamos que conectes el dispositivo a una red independiente. Puede usar Wi-Fi (como una red Wi-Fi "de invitado") o una red Ethernet independiente, preferiblemente una red física totalmente diferente. Pero una VLAN también puede proporcionar seguridad adicional. Por supuesto, este enfoque puede impedir las conexiones a los recursos o servicios de la red interna y puede requerir una configuración de red adicional para recuperar el acceso.

También se recomienda:

- Instalar actualizaciones normales del sistema
- Actualizar la configuración de Miracast para deshabilitar el modo de presentación automática

Más información

- Especificaciones de Wi-Fi Direct
- Especificación de Wireless Protected Setup (WPS)

Historial de actualizaciones de SurfaceHub

12/01/2022 • 30 minutes to read

Windows 10 diseñado para ser un servicio, lo que significa que mejora automáticamente a través de actualizaciones periódicas de software. La gran noticia es que normalmente no tiene que hacer nada para obtener las últimas actualizaciones de Windows 10, que se descargarán e instalarán siempre que estén disponibles.

La mayoría Windows actualizaciones se centran en mejoras de rendimiento y seguridad para mantenerte en funcionamiento las 24 horas del día, los 7 días de la noche.

Una cosa que escuchamos de usted es que desea saber más sobre lo que hay en nuestras actualizaciones de Windows 10, por lo que proporcionamos más detalles en esta página. En la lista siguiente, primero se muestra la actualización Windows actualización con Surface Hub mejoras específicas de la aplicación. Las actualizaciones son acumulativas, por lo que la instalación de la última actualización Windows disponible (incluso si no está en la lista siguiente) garantiza que también se beneficie de las mejoras en las actualizaciones anteriores. Microsoft Store las aplicaciones se actualizan a través del Microsoft Store (administrado por el administrador del Surface Hub del usuario). Los detalles sobre las actualizaciones de aplicaciones se proporcionan por aplicación.

Actualizaremos esta página a medida que se den a conocer nuevas actualizaciones, así que mantente al tanto de la información más reciente. Y gracias por ayudarnos a aprender y mejorar con cada actualización.

Consulte la página "Surface Hub Informaciónimportante " para temas relacionados sobre las versiones actuales y pasadas que puedan requerir su atención.

Windows 10 Team 2020 Update (20H2)

▶ 30 de septiembre de 2021: KB5004196, KB5004198 y KB5004199
▶ 30 de septiembre de 2021: actualización para Team basada en KB5005611* (compilación del sistema operativo 19042.1266)
▶ 1 de septiembre de 2021: actualización para Team basada en KB5005101* (compilación del sistema operativo 19042.1202)
▶ 29 de julio de 2021: actualización para Team basada en KB5004296* (compilación del sistema operativo 19042.1151)
▶ 10 de junio de 2021: actualización para Surface Hub 2S
▶ 13 de abril de 2021: actualización para Team basada en KB5001330* (compilación del sistema operativo 19042.928)
▶ 13 de marzo de 2021: actualización para Surface Hub 2S
▶ 2 de febrero de 2021: actualización para Team basada en KB4598291* (compilación del sistema operativo 19042.789)
▶ 15 de enero de 2021: actualización para Surface Hub 2S
▶ 11 de diciembre de 2020: actualización para Surface Hub 2S
▶ 30 de noviembre de 2020: actualización para Team basada en KB4586853* (compilación del sistema operativo 19042.662)
▶ 24 de noviembre de 2020: actualización para Surface Hub 2S
▶ 27 de octubre de 2020: actualización para Surface Hub 2S
▶ Windows 10 Team 2020 Update for Surface Hub— Notas de la versión general (compilación del sistema operativo 19042.572)

Windows 10 Team Actualización de creadores (1703)

▶ 1 de septiembre de 2020: actualización para Surface Hub 2S
▶ 4 de mayo de 2020: actualización para Surface Hub 2S
▶ 28 de febrero de 2020: actualización para Surface Hub 2S
▶ 11 de febrero de 2020: actualización para Team basada en KB4537765* (compilación del sistema operativo 15063.2284)
▶ 14 de enero de 2020: actualización para team basada en KB4534296* (compilación del sistema operativo 15063.2254)
▶ 24 de septiembre de 2019: actualización para Team basada en KB4516059* (compilación del sistema operativo 15063.2078)
▶ 17 de agosto de 2019: actualización para Team basada en KB4512474* (compilación del sistema operativo 15063.2021)
▶ 18 de junio de 2019: actualización para Team basada en KB4503289* (compilación del sistema operativo 15063.1897)
▶ 28 de mayo de 2019: actualización para Team basada en KB4499162* (compilación del sistema operativo 15063.1835)
▶ 25 de abril de 2019: actualización para Team basada en KB4493436* (compilación del sistema operativo 15063.1784)
▶ 27 de noviembre de 2018: actualización para Team basada en KB4467699* (compilación del sistema operativo 15063.1478)
▶ 18 de octubre de 2018: actualización para Team basada en KB4462939* (compilación del sistema operativo 15063.1418)
▶ 31 de agosto de 2018: actualización para Team basada en KB4343889* (compilación del sistema operativo 15063.1292)
▶ 21 de junio de 2018: actualización para Team basada en KB4284830* (compilación del sistema operativo 15063.1182)
▶ 17 de abril de 2018: actualización para Team basada en KB4093117* (compilación del sistema operativo 15063.1058)
▶ 23 de febrero de 2018: actualización para team basada en KB4077528* (compilación del sistema operativo 15063.907)
▶ 16 de enero de 2018: actualización para Team basada en KB4057144* (compilación del sistema operativo 15063.877)
▶ 12 de diciembre de 2017: actualización para Team basada en KB4053580* (compilación del sistema operativo 15063.786)
▶ 14 de noviembre de 2017: actualización para Team basada en KB4048954* (compilación del sistema operativo 15063.726)
▶ 10 de octubre de 2017: actualización para team basada en KB4041676* (compilación del sistema operativo 15063.674)
▶ 12 de septiembre de 2017: actualización para Team basada en KB4038788* (compilación del sistema operativo 15063.605)
▶ 1 de agosto de 2017: actualización para Team basada en KB4032188* (compilación del sistema operativo 15063.498)
▶ 27 de junio de 2017: actualización para Team basada en KB4022716* (compilación del sistema operativo 15063.442)
▶ 13 de junio de 2017: actualización para team basada en KB4022725* (compilación del sistema operativo 15063.413)
▶ 24 de mayo de 2017: actualización para Team basada en KB4021573* (compilación del sistema operativo 15063.328)
▶ 9 de mayo de 2017: actualización para Team basada en KB4016871* (compilación del sistema operativo 15063.296)
▶ Windows 10 Team Creators Update 1703 for Surface Hub— Notas de la versión general (compilación del sistema operativo 15063.0)

Windows 10 Team Actualización de aniversario (1607)

▶ 14 de marzo de 2017: actualización para Team basada en KB4013429* (compilación del sistema operativo 14393.953)
▶ 10 de enero de 2017: actualización para team basada en KB4000825* (compilación del sistema operativo 14393.693)
▶ 13 de diciembre de 2016: actualización para Team basada en KB3206632* (compilación del sistema operativo 14393.576)
▶ 4 de noviembre de 2016: actualización para Team basada en KB3200970* (compilación del sistema operativo 14393.447)
▶ 25 de octubre de 2016: actualización para Team basada en KB3197954* (compilación del sistema operativo 14393.351)
▶ 11 de octubre de 2016: actualización para Team basada en KB3194496* (compilación del sistema operativo 14393.222)

Actualizaciones para Windows 10 versión 1511

▶ 4 de noviembre de 2016: actualización para Team basada en KB3198586* (compilación del sistema operativo 10586.679)
▶ 12 de julio de 2016: actualización para Team basada en KB3172985* (compilación del sistema operativo 10586.494)
▶ 14 de junio de 2016: actualización para Team basada en KB3163018* (compilación del sistema operativo 10586.420)
▶ 10 de mayo de 2016: actualización para Team basada en KB3156421* (compilación del sistema operativo 10586.318)
▶ 12 de abril de 2016: actualización para Team basada en KB3147458* (compilación del sistema operativo 10586.218)

Temas relacionados

- Información de versión de Windows 10
- Windows 10 Actualización de noviembre: Preguntas frecuentes
- Historial de actualizaciones de Microsoft Surface
- Historial de actualizaciones de Microsoft Lumia
- Obtén Windows 10

Restablecer o recuperar un Surface Hub

12/01/2022 • 4 minutes to read

En este artículo se describe cómo restablecer o recuperar un Microsoft Surface Hub.

Al restablecer el Surface Hub, se devuelve su sistema operativo a la última actualización Windows acumulativa y se quitan todos los archivos de usuario locales y la información de configuración. La información que se quita incluye lo siguiente:

- La cuenta del dispositivo
- Información de cuenta para los administradores locales del dispositivo
- Información de unión a dominio o unión a Azure AD
- Información de inscripción de Administración de dispositivos móviles (MDM)
- Información de configuración que se estableció mediante MDM o la Configuración aplicación

La recuperación de Surface Hub de la nube también quita esta información. Además, el Surface Hub descarga una nueva imagen del sistema operativo e la instala. Puede especificar si el proceso de recuperación conserva otra información almacenada en el Surface Hub. La herramienta de recuperación de Surface Hub usa la misma imagen del sistema operativo si necesita recuperar una Surface Hub para la que no se puede usar ninguna de estas opciones.

Restablecer un Surface Hub

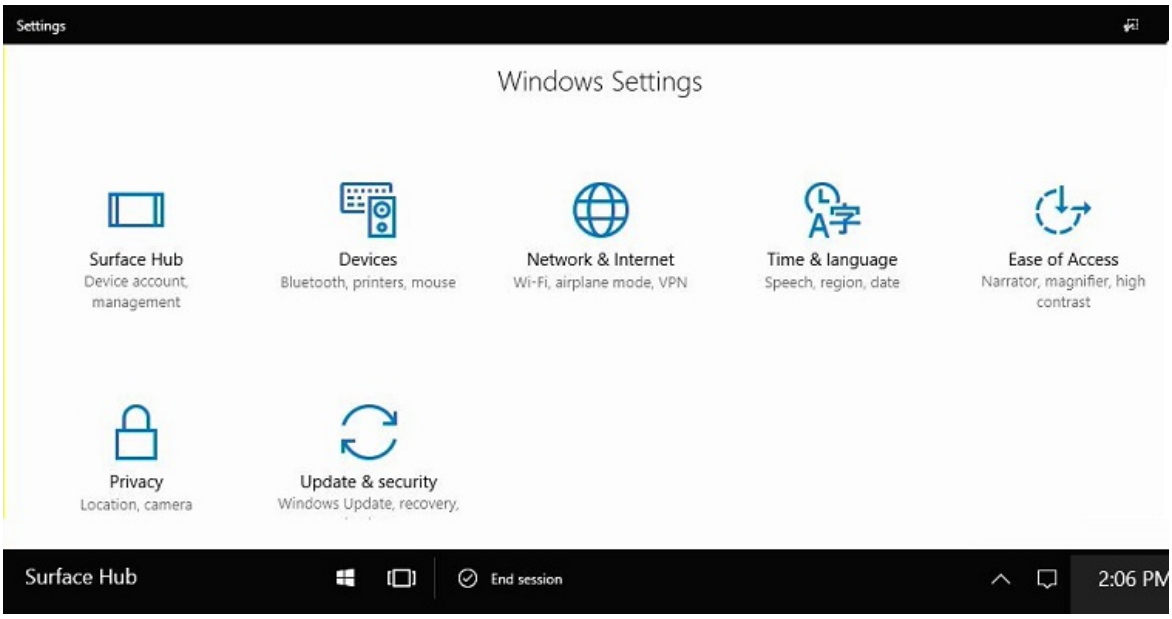
Es posible que tenga que restablecer el Surface Hub por motivos como los siguientes:

- Estás reconfigurando el dispositivo para un nuevo espacio de reuniones y quieres volver a configurarlo.
- Quieres cambiar el modo en que se administra el dispositivo de forma local.
- Se ha perdido el nombre de usuario o la contraseña de la cuenta del dispositivo o la cuenta de administrador.
- Después de instalar una actualización, el rendimiento del dispositivo disminuye.

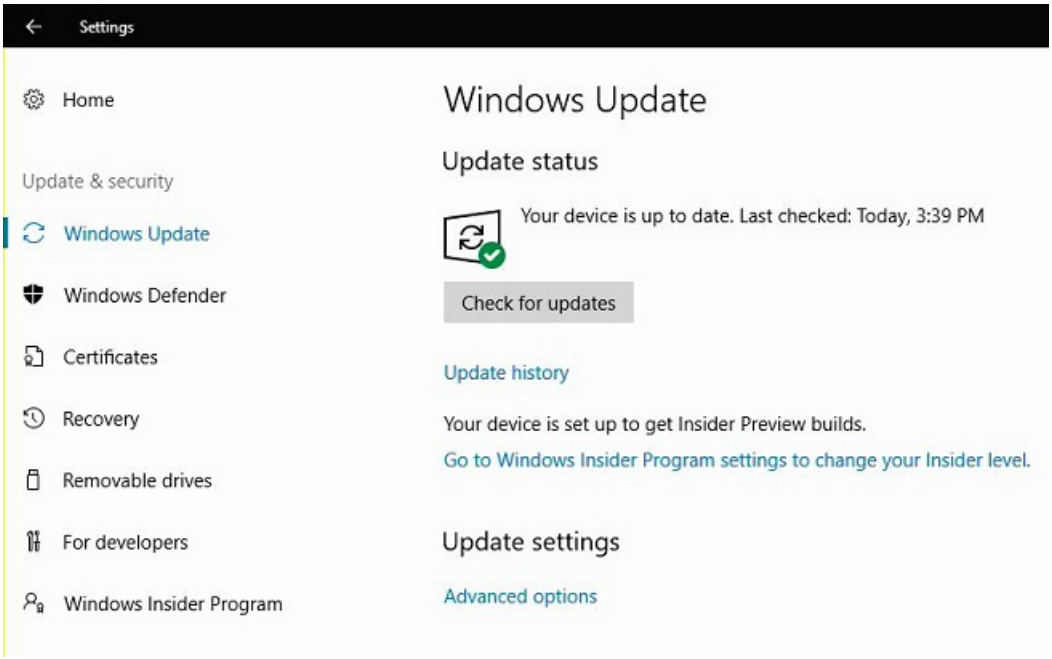
Durante el proceso de restablecimiento, si ve una pantalla en blanco durante largos períodos de tiempo, espere y no realice ninguna acción.

> **WARNING**
> El proceso de restablecimiento del dispositivo puede tardar hasta seis horas. No desactive ni desenchufe el Surface Hub hasta que el proceso haya finalizado. Si interrumpes el proceso, el dispositivo se vuelve inoperable. El dispositivo requiere el servicio de garantía para volver a funcionar.

1. En tu Surface Hub, abre **Configuración**.

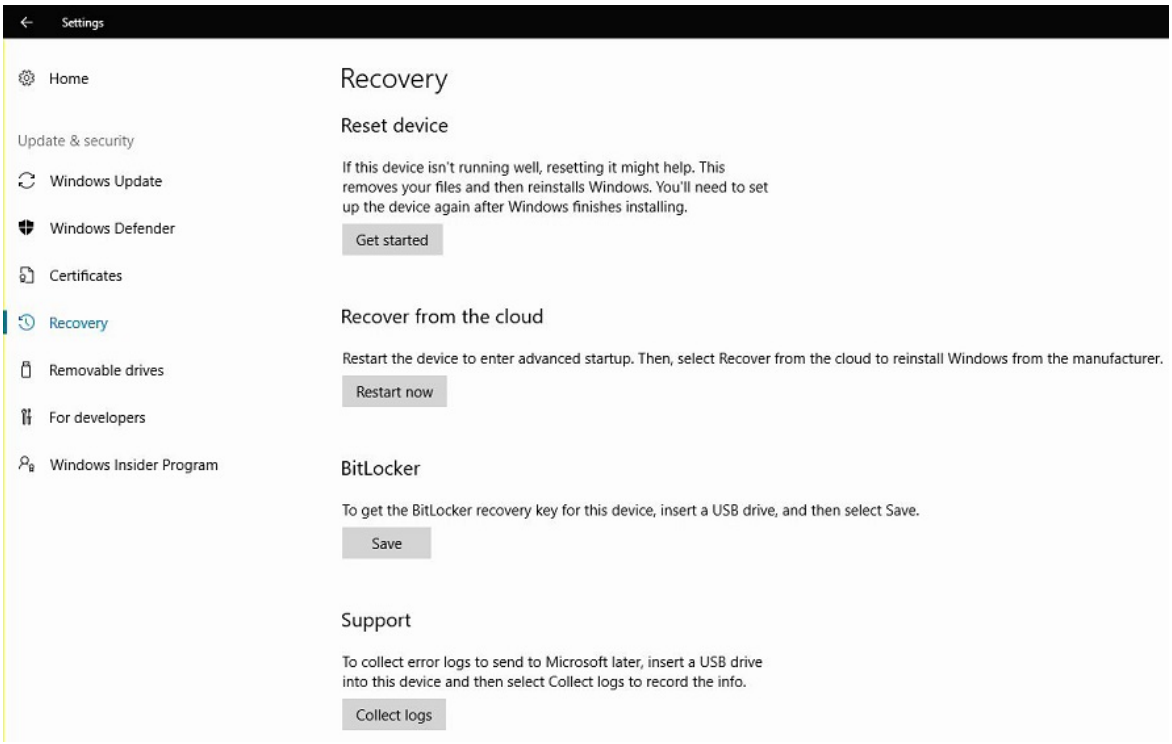


2. Seleccione **Actualizar & seguridad**.



3. Selecciona **Recuperación**y, a continuación, en **Restablecer dispositivo,** selecciona **Introducción.**

> **IMPORTANT**
>
> Asegúrate de que tienes la clave de BitLocker disponible antes de restablecer el dispositivo, como se te pedirá más adelante. Para obtener más información, consulta Guardar la clave de BitLocker. Cuando el concentrador se reinicia en la partición de recuperación, se te pedirá que escribas la clave de BitLocker. Si se omite ese mensaje, se producirá un error en el restablecimiento.



Una vez terminado el proceso de restablecimiento, el Surface Hub inicia el primer programa de ejecución de nuevo. Si el proceso de restablecimiento encuentra un problema, revierte el Surface Hub a la imagen del sistema operativo existente anteriormente y, a continuación, muestra la pantalla de bienvenida.

Recuperar un Surface Hub desde la nube

Si por algún motivo el Surface Hub se vuelve inutilizable, aún puede recuperarlo de la nube sin la ayuda del soporte técnico de Microsoft. El Surface Hub puede descargar una imagen del sistema operativo nueva de la nube y usar esa imagen para reinstalar su sistema operativo.

Es posible que tenga que usar este tipo de proceso de recuperación en las siguientes circunstancias:

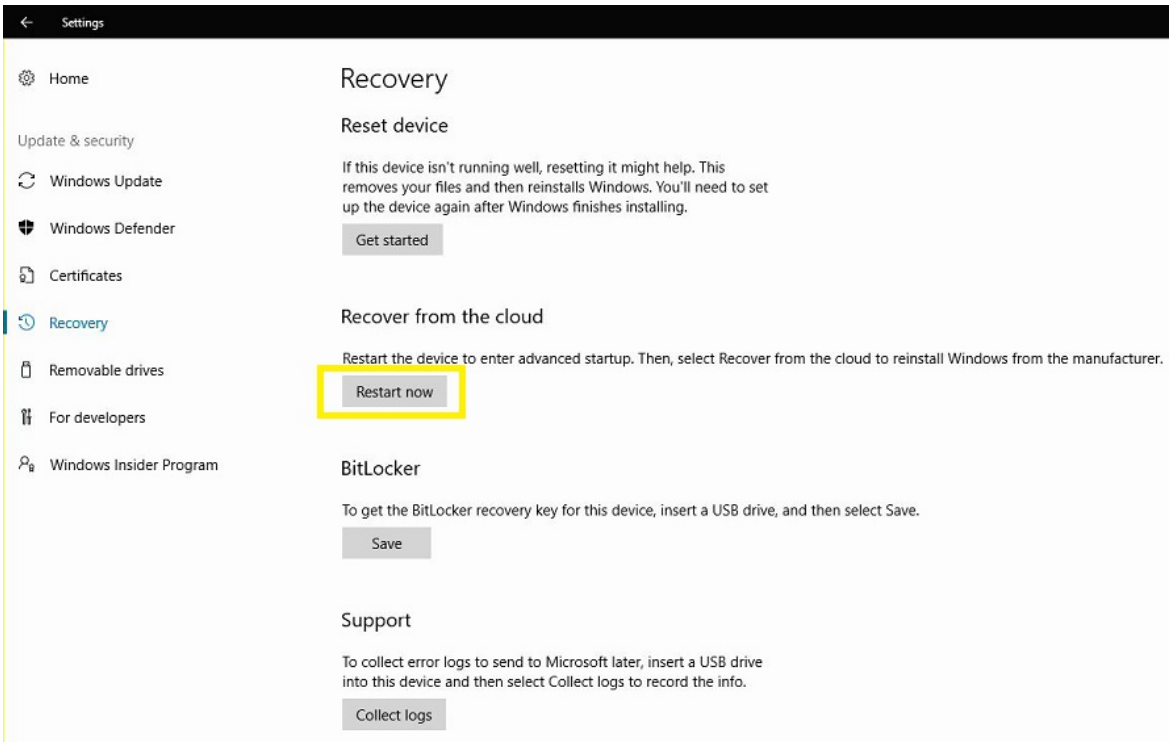
- El Surface Hub o sus cuentas relacionadas han entrado en un estado inestable
- El Surface Hub está bloqueado

> **IMPORTANT**
> El **proceso Recuperar desde la nube** requiere una conexión por cable que proporciona conectividad a Internet abierta (sin proxy u otros mensajes de autenticación).

Recuperar un Surface Hub de un estado defectuoso

Si la cuenta del dispositivo entra en un estado inestable o si la cuenta de administrador tiene problemas, puedes usar la aplicación Configuración para iniciar el proceso de recuperación en la nube. Solo debes usar el proceso de recuperación en la nube cuando el proceso de restablecimiento del dispositivo no solucione el problema.

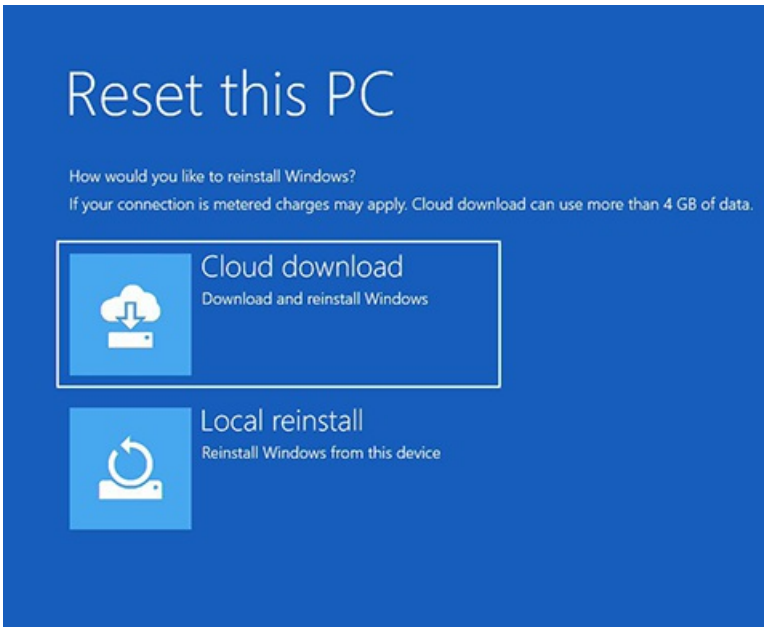
1. En el Surface Hub, seleccione **Configuración** > **Actualizar & de** > **seguridad**.
2. En **Recuperar desde la nube,** seleccione Reiniciar **ahora**.



Recuperar un Surface Hub bloqueado

En raras ocasiones, un Surface Hub puede producir un error al limpiar los datos de usuario y de la aplicación al final de una sesión. Cuando esto sucede, el dispositivo se reinicia automáticamente e intenta de nuevo la operación. Pero si esta operación falla repetidamente, el dispositivo se bloquea automáticamente para proteger los datos del usuario. Para desbloquearlo, debes restablecer el dispositivo o, si no funciona, recuperarlo de la nube.

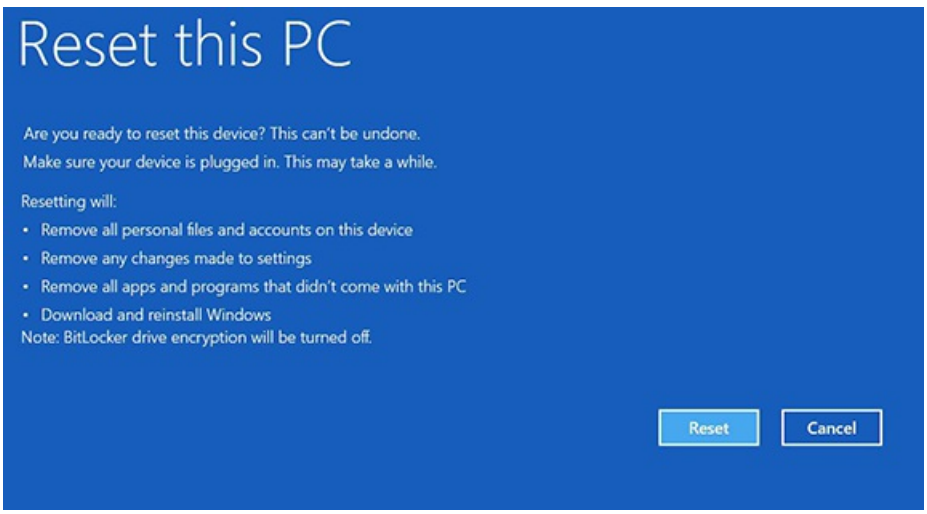
1. Busque el conmutador de alimentación en la parte inferior de Surface Hub. El conmutador de alimentación está junto a la conexión del cable de alimentación. Para obtener más información acerca del conmutador de alimentación, consulte la Surface Hub guía de preparación del sitio (PDF).
2. Mientras el Surface Hub muestra la pantalla de bienvenida, use el conmutador de alimentación para desactivar el Surface Hub.
3. Use el conmutador de alimentación para volver a activar Surface Hub la red. El dispositivo se inicia y muestra la Surface Hub logotipo. Cuando veas puntos giratorios debajo del logotipo de Surface Hub, usa el conmutador de energía para volver a desactivar Surface Hub.
4. Repita el paso 3 tres veces o hasta que Surface Hub muestra el mensaje "Preparación de reparación automática". Después de mostrar este mensaje, el Surface Hub muestra la Windows RE pantalla.
5. Seleccione **Restablecer**.
6. Si se te pide que escribas la clave de BitLocker, sigue uno de estos procedimientos:
   - Para conservar la información que BitLocker protege en el Surface Hub, escriba la clave de BitLocker.
   - Para descartar la información protegida, seleccione Omitir esta unidad
7. Seleccione **Descarga en la nube.**



> **IMPORTANT**
>
> Si recibe un mensaje de error que indica **No se puede descargar**, seleccione **Cancelar** y, a continuación, **Restablecer de** nuevo.

8. Seleccione **Limpiar completamente la unidad.**

9. Se te **preguntará ¿Estás listo para restablecer este dispositivo?**. Seleccione **Restablecer**.



10. La descarga comienza y el proceso de recuperación indica **restablecer este dispositivo**.

Contactar con el soporte técnico

Si tiene preguntas o necesita ayuda, puede crear una solicitud de soporte técnico.

Temas relacionados

Administrar Microsoft Surface Hub

Guía del administrador de Microsoft Surface Hub

Uso de la herramienta de recuperación de Surface Hub

12/01/2022 • 4 minutes to read

La herramienta de recuperación de Microsoft Surface Hub ayuda a volver a crear una imagen de la unidad de estado sólido (SSD) de Surface Hub con un dispositivo de escritorio Windows 10, sin llamar al soporte técnico ni reemplazar el SSD. Con esta herramienta, puedes volver a crear una imagen de un SSD que tiene una contraseña de administrador desconocida, errores de arranque, no pudo completar una recuperación en la nube o para un dispositivo que tiene una versión anterior del sistema operativo. La herramienta no corregirá los SSD dañados físicamente.

Para volver a crear una imagen de la SSD de Surface Hub con la herramienta de recuperación, deberá quitar el SSD del Surface Hub, conectar la unidad al cable USB a SATA y, a continuación, conectar el cable al equipo de escritorio en el que está instalada la herramienta de recuperación. Para obtener más información sobre cómo quitar la unidad existente de su Surface Hub, vea Surface Hub reemplazo de SSD.

> **IMPORTANT**
> No deje que el dispositivo se ponga en reposo ni interrumpa la descarga del archivo de imagen.

Si la herramienta no ha sido correcta al reimaging de la unidad, póngase en contacto Surface Hub soporte técnico.

Requisitos previos

Mandatory

- Equipo host que ejecuta una versión de 64 bits de Windows 10 versión 1607 o posterior.
- Acceso a Internet
- Abrir puerto USB 2.0 o posterior
- Cable USB a SATA
- 10 GB de espacio libre en disco en el equipo host
- Ssd enviados con Surface Hub ssd proporcionados por el soporte técnico como reemplazo. Los SSD no proporcionados por Microsoft no son compatibles.

Recomendaciones

- Conexión a Internet de alta velocidad
- Abrir puerto USB 3.0
- Cable USB 3.0 o superior USB a SATA
- La herramienta de creación de imágenes se ha probado con la siguiente creación y modelo de cables:
  - Startech USB312SAT3CB
  - Rosewill RCUC16001
  - Ugreen 20231

Descargar Surface Hub recuperación

Surface Hub Recovery Tool está disponible para su descarga desde Surface Hub Tools for IT bajo el nombre de archivo **SurfaceHub_Recovery_v2.7.139.0.msi**.

IMPORTANT

Esta versión, publicada el 11 de febrero de 2021, reemplaza a la compilación anterior, que ya no es funcional. Si descargó esta herramienta anteriormente, desinstale e instale la versión actual.

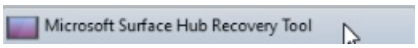
Para iniciar la descarga, haga clic **en Descargar**, ** elijaSurfaceHub_Recovery_v2.7.139.0.msi** de la lista y haga clic en **Siguiente**. En la ventana emergente, elija una de las siguientes opciones:

- Haga **clic en** Ejecutar para iniciar la instalación inmediatamente.
- Haga **clic en** Guardar para copiar la descarga en el equipo para su instalación posterior.

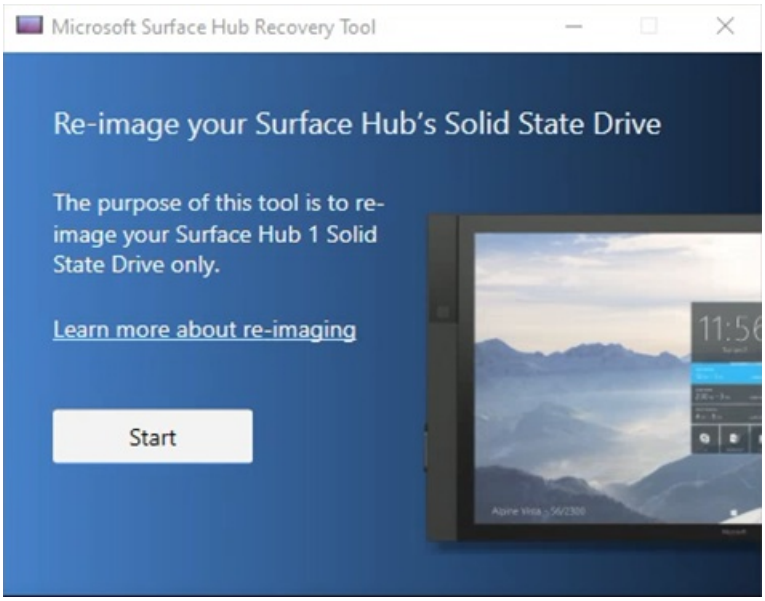
Instalar Surface Hub recuperación en el equipo host.

Ejecutar Surface Hub recuperación

1. En el equipo host, seleccione **el** botón Inicio, desplácese por la lista alfabética de la izquierda y seleccione el acceso directo de la herramienta de recuperación.

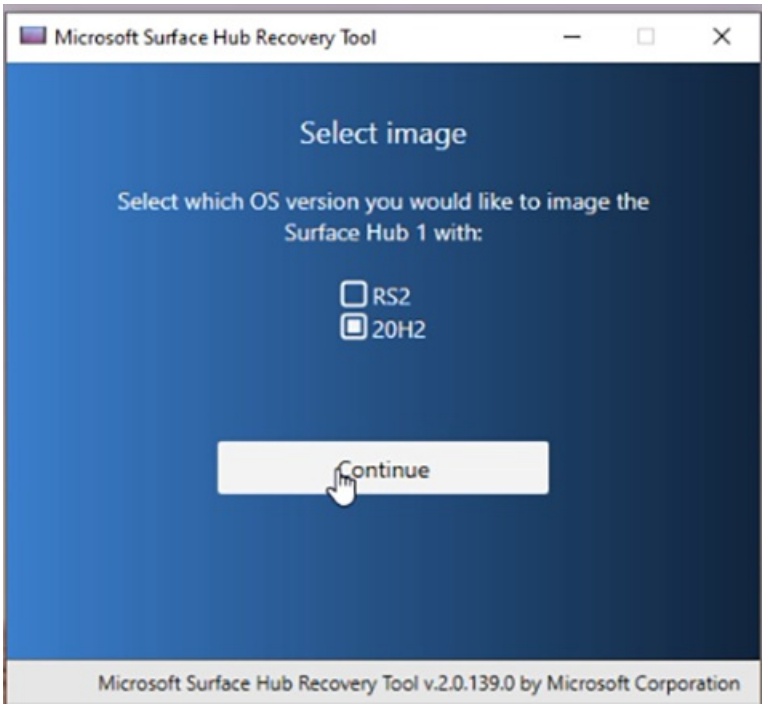


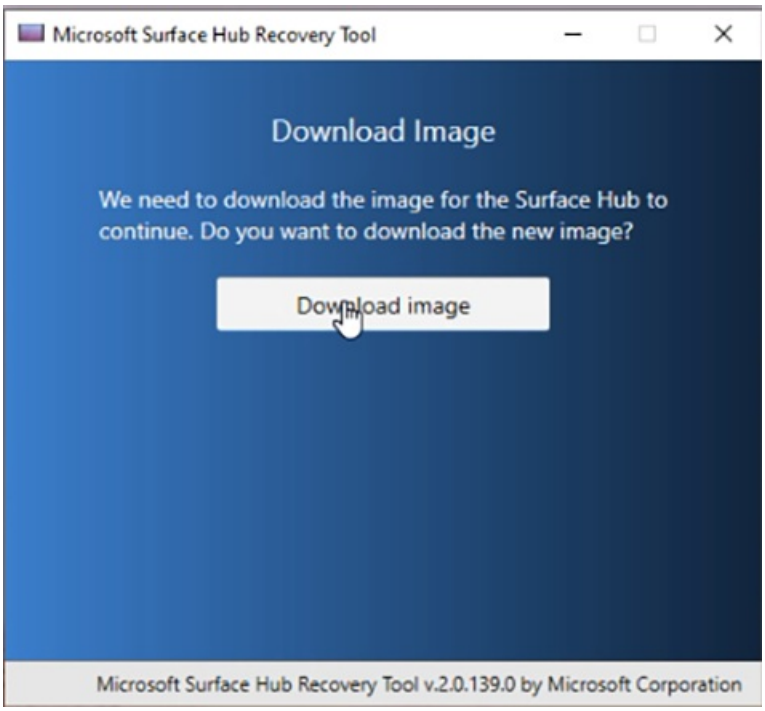
2. Haz clic en **Inicio**.



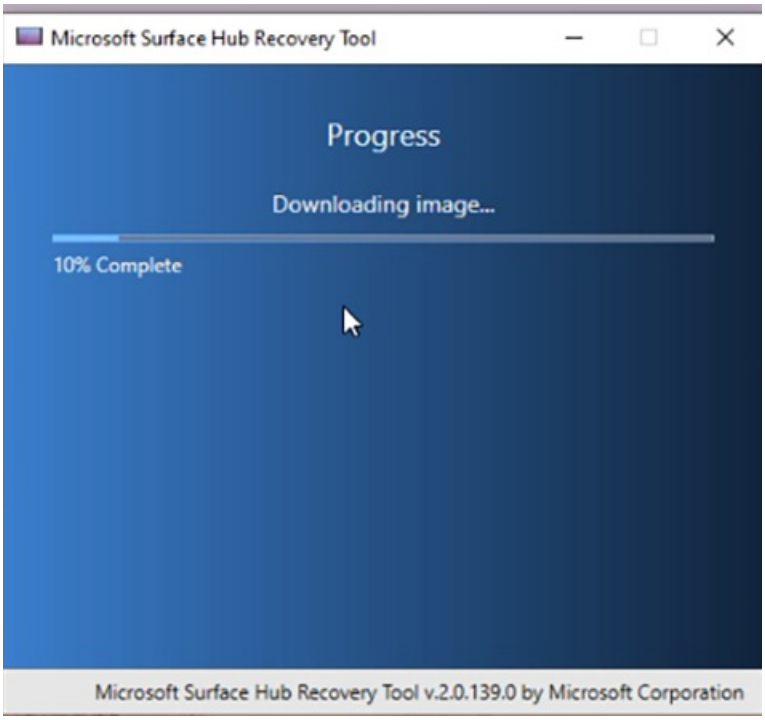
3. En la **ventana Guía,** haga clic **en Siguiente**.

4. En la ventana Seleccionar imagen, haga clic en **RS2** o en su **sucesor 20H2,** seleccione **Continuar y,** a continuación, **seleccione Descargar imagen.**

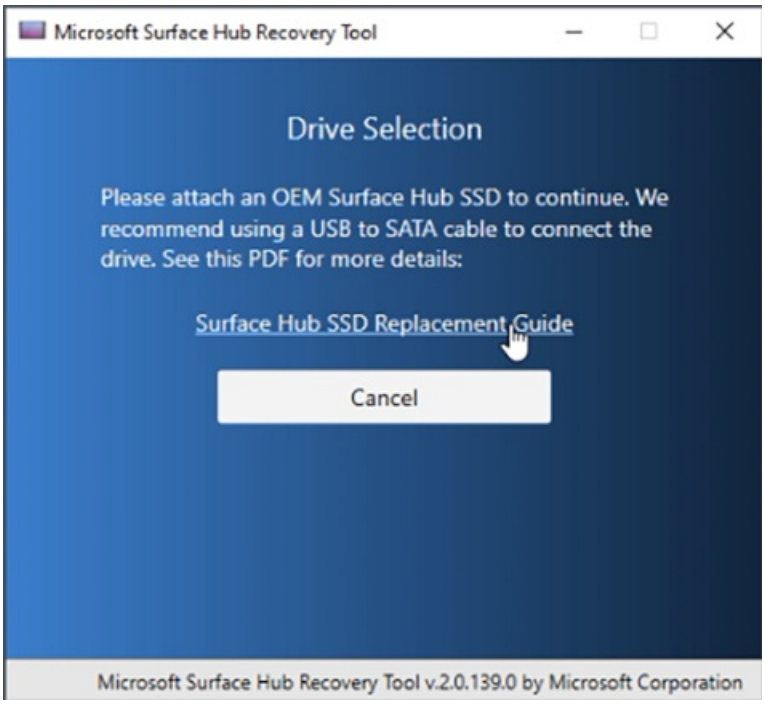




5. El tiempo para descargar la imagen de recuperación depende de las velocidades de conexión a Internet. En una conexión corporativa promedio, puede tardar hasta una hora en descargar el archivo de imagen de 8 GB.



6. Una vez completada la descarga, la herramienta le indica que conecte una unidad SSD. Si la herramienta no puede localizar la unidad adjunta, es muy posible que el cable que se usa no informe del nombre del SSD a Windows. La herramienta de creación de imágenes debe encontrar el nombre de la unidad como "Dispositivo USB LITEON L CH-128V2S" para poder continuar. Para obtener más información sobre cómo quitar la unidad existente de su Surface Hub, vea Surface Hub reemplazo de SSD.



7. Cuando se reconozca la unidad, haga clic **en Inicio** para iniciar el proceso de re-creación de imágenes. En la advertencia de que se borrarán todos los datos de la unidad, haga clic en **Aceptar**.

   Antes de aplicar la imagen del sistema a la unidad, el SSD se vuelve a particionar y dar formato. Copiar los archivos binarios del sistema llevará aproximadamente 30 minutos, pero puede tardar más en función de la velocidad del bus USB, el cable que se usa o el software antivirus instalado en el sistema.

Solución de problemas y problemas comunes

PROBLEMA	NOTAS
La herramienta no puede crear una imagen del SSD	Asegúrese de usar un SSD suministrado de fábrica y uno de los cables probados.
El proceso de reimplante aparece detenido o inmovilizado	Es seguro cerrar y reiniciar la herramienta de Surface Hub recuperación sin ningún efecto negativo para la SSD.
La herramienta no reconoce la unidad	Compruebe que el SSD Surface Hub está enumerado como una unidad Lite-On, "Liteon L CH-128V2S USB Device". Si la unidad se reconoce como otro dispositivo con nombre, el cable actual no es compatible. Pruebe otro cable o uno de los cables probados enumerados anteriormente.
Error: -2147024809	Abra el Administrador de discos y quite las particiones de la Surface Hub disco. Desconecte y vuelva a conectar la unidad al equipo host. Reinicie la herramienta de creación de imágenes de nuevo.

Si la herramienta no ha sido correcta al reimaging de la unidad, póngase en contacto Surface Hub soporte técnico.

Historial de versiones

Versión v2.7.139.0

Fecha de lanzamiento: 11 de febrero de 2021

Esta versión de Surface Hub Recovery Tool agrega compatibilidad con lo siguiente:

- Actualización de seguridad

Versión v2.0.139.0

> **IMPORTANT**
>
> Esta versión ya no es funcional. Descargue la versión actual, enumerada anteriormente.

Fecha de lanzamiento: 18 de diciembre de 2020

Esta versión de Surface Hub Recovery Tool agrega compatibilidad con lo siguiente:

- Actualización para admitir Windows 10 Team 2020 Update (20H2)
- Mejoras en la experiencia del usuario
- Cambios en la arquitectura
- Adiciones de telemetría

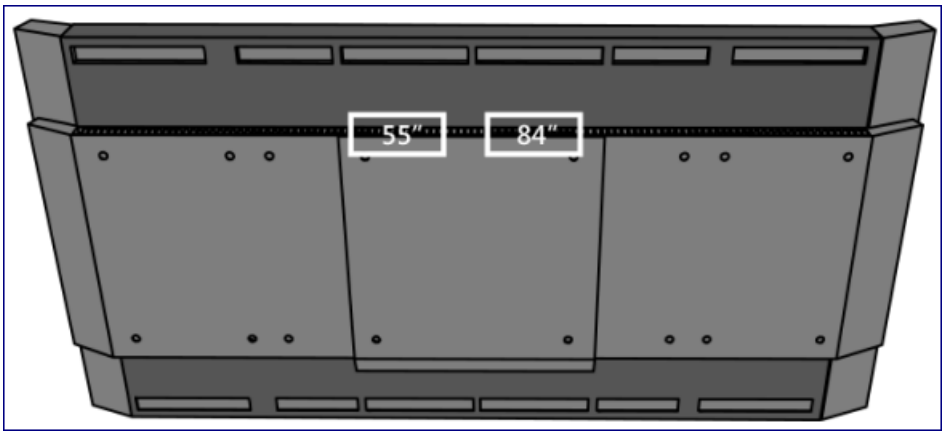
Reemplazo de SSD de Surface Hub

12/01/2022 • 2 minutes to read

Es posible que deba quitar la unidad de estado sólido (SSD) de su Surface Hub para poder volver a crearla con la herramienta de recuperación de Surface Hub o porque se le envió una unidad de reemplazo. Volver a crear una imagen de ssd cuando el sistema operativo ya no se puede arrancar, como un error de actualización de Windows, problemas de BitLocker, un error de restablecimiento o un error de hardware.

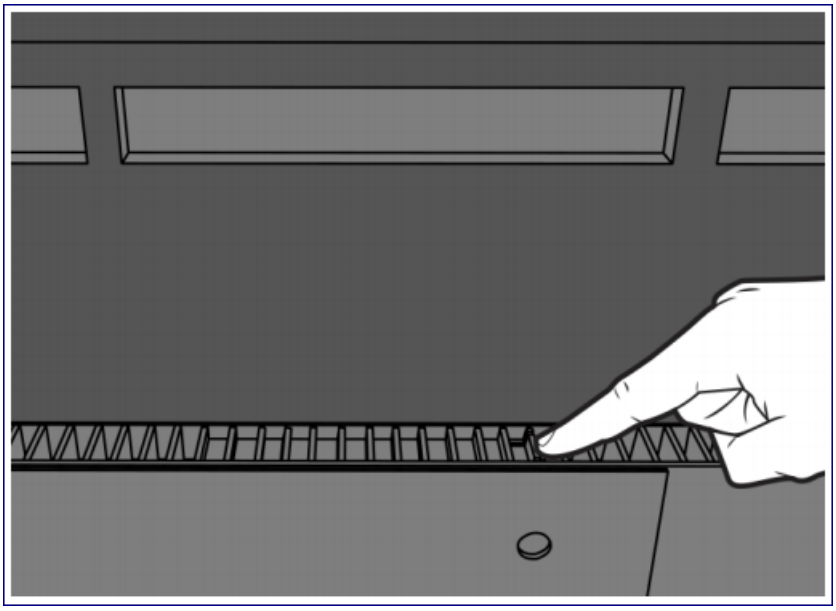
> **WARNING**
> Asegúrese de que la Surface Hub esté desactivada en el conmutador de CA.

1. Busque la puerta del compartimento SSD en la parte superior de la Surface Hub en las ubicaciones que se muestran a continuación. La puerta es identificable, ya que no tiene ranuras de ventilación abiertas.



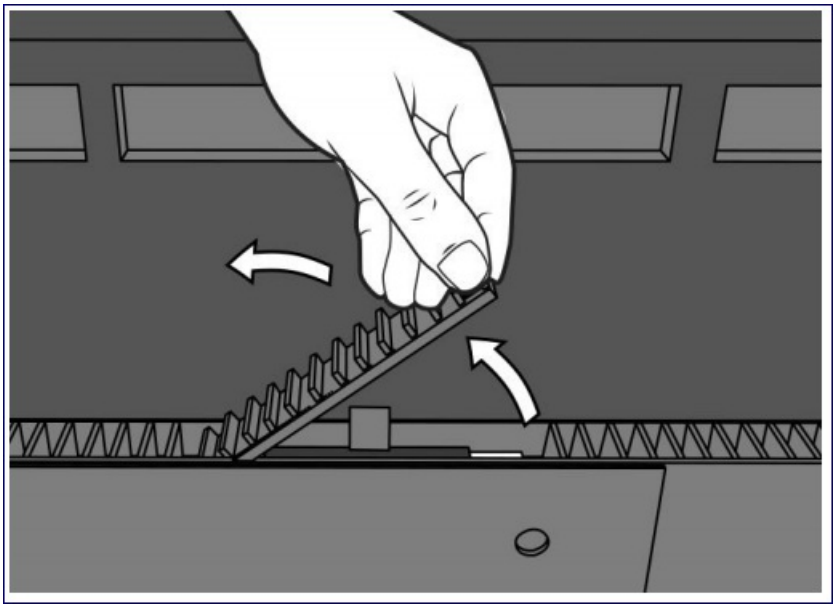
Surface Hub de disco duro

2. Busque la pestaña de bloqueo en la puerta del compartimento del disco duro. En el Surface Hub 55, la pestaña de bloqueo se ubicará en el lado izquierdo de la puerta. En la Surface Hub 84, estará en el lado derecho, como se muestra en la ilustración.



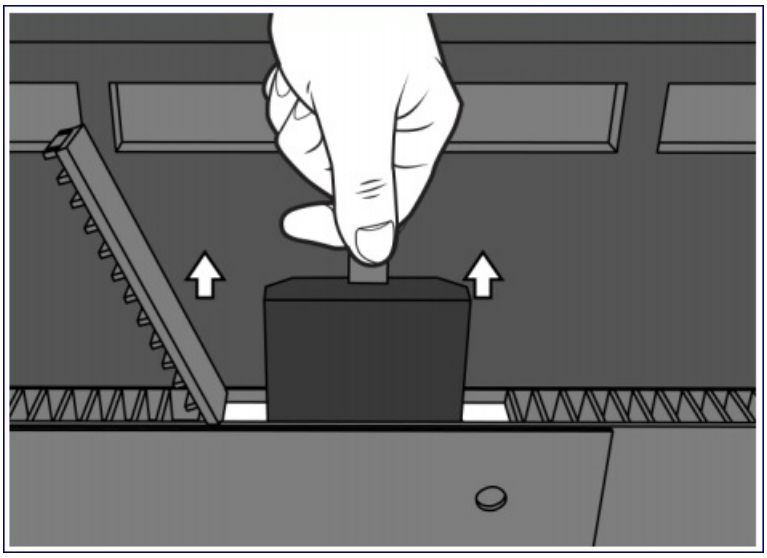
Pestaña de bloqueo en la puerta del compartimento del disco duro

3. Levante la puerta del compartimento para acceder al disco duro.



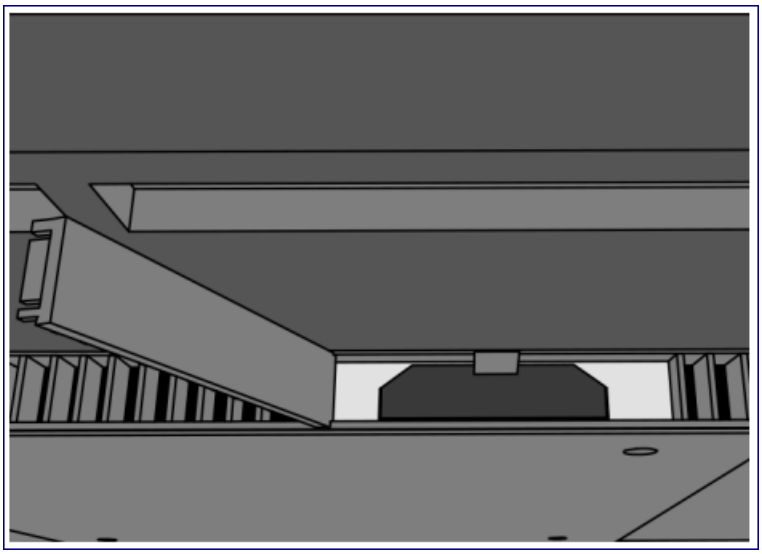
Puerta del compartimento de elevación

4. Busque la pestaña de extracción, que puede estar parcialmente oculta debajo de la cubierta posterior. Tira de la pestaña para expulsar la unidad de disco duro del compartimento.



Pestaña Extraer

5. Deslice la unidad de reemplazo en su lugar hasta que oiga que haga clic.



Unidad de reemplazo de diapositivas en su lugar

6. Cierre la puerta del compartimento.
7. Aplique energía al Surface Hub.

Soluciones principales de soporte técnico para Microsoft SurfaceHub

12/01/2022 • 2 minutes to read

Microsoft publica periódicamente actualizaciones y soluciones para dispositivos SurfaceHub. Para garantizar que los dispositivos pueden recibir actualizaciones futuras, incluidas las actualizaciones de seguridad, es importante mantener los dispositivos SurfaceHub actualizados. Para obtener una lista completa del historial de actualizaciones, consulta Historial de actualizaciones de Surface Hub y Problemas conocidos e información adicional sobre Microsoft Surface Hub.

> **TIP**
> ¿Buscas información de garantía de Surface Hub?

Estas son las mejores soluciones del Soporte técnico de Microsoft para problemas comunes experimentados con dispositivos Surface Hub.

Problemas de configuración e instalación

- Solución de problemas de configuración
- Errores de Exchange ActiveSync

Problemas de Miracast

- Solucionar problemas de Miracast en Surface Hub

Problemas para descargar actualizaciones

- Surface Hub no puede descargar actualizaciones de Windows Update

Problemas para conectar aplicaciones

- La aplicación Connect de Surface Hub se cierra inesperadamente

Solucionar problemas de Microsoft Surface Hub

12/01/2022 • 12 minutes to read

Solucionar problemas comunes, incluidos los problemas de instalación y errores de Exchange ActiveSync.

La herramienta Diagnóstico de hardware de SurfaceHub incluye pruebas interactivas que te permiten confirmar que la funcionalidad esencial del hub esté funcionando según lo previsto. Además de probar el hardware, el diagnóstico puede probar la cuenta de recursos para comprobar si está configurada correctamente para tu entorno. Si surgen problemas, los resultados se pueden guardar y compartir con el equipo de soporte técnico de SurfaceHub. Para obtener información de uso, consulta Uso de la herramienta de diagnóstico de hardware de Surface Hub para probar una cuenta del dispositivo.

Los problemas comunes se enumeran en la siguiente tabla, junto con las causas y las posibles soluciones. La sección Solución de problemas del programa de instalación contiene una lista de problemas en el dispositivo, junto con varios tipos de problemas que se pueden encontrar durante la experiencia de primera ejecución. La sección Errores de Exchange ActiveSync enumera errores comunes que el dispositivo puede encontrar al intentar sincronizarse con un servidor Microsoft Exchange ActiveSync.

Solución de problemas del programa de instalación

Esta sección enumera las causas y posibles correcciones para ayudar a solucionar problemas que puedes encontrar al configurar el Microsoft Surface Hub.

En el dispositivo

Posibles correcciones para los problemas del Surface Hub después de haber completado el programa de primera ejecución.

PROBLEMA	CAUSAS	POSIBLES SOLUCIONES
No recibir mensajes de aceptar o rechazar automáticamente.	La cuenta del dispositivo no está configurada para aceptar o rechazar mensajes automáticamente.	Usar el cmdlet de PowerShell `Set-CalendarProcessing $upn -AutomateProcessing AutoAccept` .
	La cuenta del dispositivo no está configurada para procesar convocatorias de reunión externas.	Usar el cmdlet de PowerShell `Set-CalendarProcessing $upn -ProcessExternalMeetingMessages $true` .
El calendario no se muestra en la pantalla de bienvenida o se está mostrando el mensaje "Citas de fecha (ninguna cuenta aprovisionada)".	No hay ninguna cuenta del dispositivo configurada en este Surface Hub.	Proporcionar una cuenta del dispositivo a través Configuración.

El calendario no se muestra en la pantalla de bienvenida o se está mostrando el mensaje "Citas de fecha (sobreaprovisionadas)".	La cuenta del dispositivo está aprovisionada en demasiados dispositivos.	Quitar la cuenta del dispositivo de otros dispositivos a los que esté aprovisionada. Esto se puede realizar mediante el portal de administración de Exchange.
El calendario no se muestra en la pantalla de bienvenida o se está mostrando el mensaje "Citas de fecha (credenciales no válidas)".	La contraseña de la cuenta del dispositivo ha expirado y ya no es válida.	Actualizar la contraseña de la cuenta en Configuración. Consulta también Administración de contraseñas.
El calendario no se muestra en la pantalla de bienvenida o se está mostrando el mensaje "Citas de fecha (directiva de cuenta)".	La cuenta del dispositivo está usando una directiva de ActiveSync no válida.	Asegúrate de que la cuenta del dispositivo tiene una directiva de ActiveSync donde `PasswordEnabled == False`.
El calendario no se muestra en la pantalla de bienvenida o se está mostrando el mensaje "Las citas pueden estar desactualizadas".	Exchange no está habilitado.	Habilitar la cuenta del dispositivo para los servicios de Exchange mediante Configuración. Debes asegurarte de que tienes el conjunto de directivas de ActiveSync correcto y de que has instalado también los certificados necesarios para que los servicios de Exchange funcionen.
No se puede iniciar sesión en Skype Empresarial.	La cuenta del dispositivo no tiene una propiedad de dirección de Protocolo de inicio de sesión (SIP).	La cuenta no tiene una propiedad de dirección SIP y su Nombre principal de usuario (UPN) no coincide con la dirección SIP real. La cuenta debe tener su dirección SIP establecida, o bien debería agregarse la dirección SIP mediante la aplicación Configuración.
No se puede iniciar sesión en Skype Empresarial.	La cuenta del dispositivo requiere un certificado para autenticarse en Skype Empresarial.	Instalar el certificado apropiado mediante el aprovisionamiento de paquetes.

Primera ejecución

Correcciones posibles para los problemas con el programa de primera ejecución de Surface Hub.

PROBLEMA	CAUSAS	POSIBLES SOLUCIONES
No se encuentra la cuenta al pedir el dominio y el nombre de usuario.	El dominio debe ser el nombre de dominio completo (FQDN).	Debe proporcionarse el FQDN en el campo de dominio.

Página de la cuenta del dispositivo, problemas de configuración de la cuenta nueva

PROBLEMA	CAUSAS	POSIBLES SOLUCIONES
No se pudo encontrar la cuenta proporcionada en Azure AD.	El Nombre principal de usuario (UPN) de la cuenta proporcionada tiene un inquilino con el que no se puede contactar en Azure AD.	Asegúrate de que tienes una conexión a Internet activa y de que el dispositivo puede contactar con Microsoft Online Services. Asegúrate de que las credenciales de cuenta se han escrito correctamente.
No se puede alcanzar el directorio especificado.	El dominio de la cuenta proporcionada especifica un dominio que no se puede alcanzar.	Asegúrate de que tienes una conexión de red en funcionamiento y de que el dispositivo puede alcanzar el controlador de dominio. Asegúrate de que las credenciales de cuenta se han escrito correctamente. También puedes intentar usar el FQDN en su lugar.
No se puede detectar automáticamente el servidor Exchange.	El servidor Exchange no está configurado para la detección automática.	Habilita la detección automática del servidor Exchange para la cuenta del dispositivo o escribe la dirección del servidor Exchange de la cuenta manualmente.
No se pudo detectar la dirección SIP después de escribir las credenciales de cuenta.	No había ninguna entrada de dirección SIP en Active Directory o Azure AD.	Asegúrate de que la cuenta está habilitada con Skype Empresarial y de que tiene una dirección SIP. Si no es así, puedes escribir la dirección SIP de forma manual en el cuadro de texto.

Página de la cuenta del dispositivo, problemas de configuración de cuentas existentes

PROBLEMA	CAUSAS	CÓDIGOS DE ERROR	POSIBLES SOLUCIONES
No se pudo autenticar la cuenta con las credenciales especificadas.	La cuenta no está habilitada como un usuario en Active Directory (AD), necesita una contraseña para su autenticación o la contraseña es incorrecta.	Ninguno	Asegúrate de que las credenciales se han escrito correctamente. Habilita la cuenta como un usuario en AD y agrega una contraseña o establece RoomMailboxPassword .
Se muestra el error 0x800C0019 al proporcionar un servidor Exchange.	La cuenta del dispositivo requiere un certificado para autenticarse.	0x800C0019	Instalar el certificado apropiado mediante el aprovisionamiento de paquetes.

Las credenciales de cuenta del dispositivo no son válidas para el servidor Exchange proporcionado.	El servidor Exchange proporcionado no se encuentra donde se hospeda el buzón de la cuenta del dispositivo.	Ninguno	Asegúrate de que estás proporcionando el servidor de correo de Exchange correcto para la cuenta del dispositivo.
Se agotó el tiempo de espera HTTP al intentar alcanzar el servidor Exchange.		0x80072EE2	
No se pudo encontrar el servidor Exchange proporcionado.	No se pudo encontrar el servidor Exchange proporcionado.	Ninguno	Asegúrate de que tienes una red en funcionamiento o conexión a Internet y de que el servidor Exchange que proporcionaste es correcto.
HTTP no compatible.	Se proporcionó un servidor Exchange con *http://* en lugar de *https://*.	Ninguno	Usar un servidor Exchange que usa https.
Los usuarios llegan a la página titulada "Hay un problema con esta cuenta" en relación con ActiveSync.	La directiva PasswordEnabled de ActiveSync está establecida en True (o 1).	Ninguno	Crear una nueva directiva de ActiveSync en la que PasswordEnabled esté establecida en False (o 0) y, a continuación, aplica esa directiva a la cuenta.
	El Surface Hube no tiene una conexión con Exchange.	Ninguno	Asegúrate de que tienes una red en funcionamiento o conexión a Internet.
	Exchange devuelva un código de estado que indique un error.	Ninguno	Asegúrate de que tienes una red en funcionamiento o conexión a Internet.

Primera ejecución, problemas de la página de unión a un dominio

PROBLEMA	CAUSAS	POSIBLES SOLUCIONES
Al intentar unirte a un dominio, se muestra un error por el que la cuenta no se pudo autenticar con las credenciales especificadas.	Las credenciales proporcionadas no se pueden unir al dominio especificado.	Escribe las credenciales correctas de una cuenta que exista en el dominio especificado.
Al especificar un grupo desde un dominio, se muestra un error por el que no se encontró el grupo en el dominio.	Es posible que el grupo se haya quitado o que ya no exista.	Comprueba que el grupo existe en el dominio.

Primera ejecución, página del servidor Exchange

PROBLEMA	CAUSAS	POSIBLES SOLUCIONES
Los usuarios llegan a esta página y se les pide la dirección del servidor Exchange.	El servidor Exchange no está configurado para la detección automática.	Habilita la detección automática del servidor Exchange para la cuenta del dispositivo o escribe la dirección del servidor Exchange de la cuenta manualmente.

Primera ejecución, problemas en el dispositivo

PROBLEMA	CAUSAS	CÓDIGOS DE ERROR	POSIBLES SOLUCIONES
No se pueden sincronizar el correo ni el calendario.	La cuenta no estableció el Surface Hub como un dispositivo permitido.	0x86000C1C	Para agregar el identificador de dispositivo de Surface Hub a la lista de permitidos, establece la propiedad ActiveSyncAllowedDeviceIds para el buzón.

Errores de Exchange ActiveSync

En esta sección se muestran los códigos de estado, la asignación, los mensajes de usuario y las acciones que un administrador puede realizar para solucionar errores de Exchange ActiveSync.

CÓDIGO HEXADECIMAL	ASIGNACIÓN	MENSAJE DESCRIPTIVO	ACCIONES QUE DEBE REALIZAR EL ADMINISTRADOR
0x85010002	E_HTTP_DENIED	Se debe actualizar la contraseña.	Actualizar la contraseña.

CÓDIGO HEXADECIMAL	ASIGNACIÓN	MENSAJE DESCRIPTIVO	ACCIONES QUE DEBE REALIZAR EL ADMINISTRADOR
0x80072EFD	WININET_E_CANNOT_CONNECT	No se puede conectar al servidor en este momento. Espera unos instantes y vuelve a intentarlo o comprueba la configuración de la cuenta.	Comprueba que el nombre del servidor es correcto y accesible. Comprueba que el dispositivo está conectado a la red.
0x86000C29	E_NEXUS_STATUS_DEVICE_NOTPROVISIONED (las directivas no coinciden)	La cuenta está configurada con directivas que no son compatibles con Surface Hub.	Deshabilitar la directiva **PasswordEnabled** para esta cuenta. Se ha producido un error que se producía un error en la política si la cuenta no recibe notificaciones del servidor en el intervalo de actualización de la Directiva.
0x86000C4C	E_NEXUS_STATUS_MAXIMUMDEVICESREACHED	La cuenta tiene demasiadas asociaciones de dispositivo.	Elimina una o más asociaciones en el servidor.
0x86000C0A	E_NEXUS_STATUS_SERVERERROR_RETRYLATER	No se puede conectar al servidor en este momento.	Espera a que el servidor vuelva a estar conectado. Si el problema persiste, vuelve a aprovisionar la cuenta.
0x85050003	E_CREDENTIALS_EXPIRED (las credenciales expiraron y deben actualizarse)	Se debe actualizar la contraseña.	Actualizar la contraseña.
0x8505000D	E_AIRSYNC_RESET_RETRY	No se puede conectar al servidor en este momento. Espera un momento o verifica la configuración de la cuenta.	Esto suele ser un error transitorio, pero si el problema persiste, comprueba el número de dispositivos asociados con la cuenta y elimina algunos de ellos si el número es grande.
0x86000C16	E_NEXUS_STATUS_USER_HASNOMAILBOX	El buzón se migró a un servidor diferente.	Nunca deberías ver este error. Si el problema persiste, vuelve a aprovisionar la cuenta.

CÓDIGO HEXADECIMAL	ASIGNACIÓN	MENSAJE DESCRIPTIVO	ACCIONES QUE DEBE REALIZAR EL ADMINISTRADOR
0x85010004	E_HTTP_FORBIDDEN	No se puede conectar al servidor en este momento. Espera un momento e inténtalo de nuevo, o verifica la configuración de la cuenta.	Comprueba el nombre del servidor para asegurarse de que es correcto. Si la cuenta está usando una autenticación basada en certificados, asegúrate de que el certificado sigue siendo válido y actualízalo si no es el caso.
0x85030028	E_ACTIVESYNC_PASSWORD_OR_GETCERT	Falta o no es válida la contraseña de la cuenta o el certificado de cliente.	Actualiza la contraseña o implementa el certificado de cliente.
0x86000C2A	E_NEXUS_STATUS_DEVICE_POLICYREFRESH	La cuenta está configurada con directivas que no son compatibles con Surface Hub.	Deshabilitar la directiva PasswordEnabled para esta cuenta.
0x85050002	E_CREDENTIALS_UNAVAILABLE	Se debe actualizar la contraseña.	Actualizar la contraseña.
0x80072EE2	WININET_E_TIMEOUT	La red no es compatible con el tiempo de espera mínimo de inactividad requerido para recibir la notificación del servidor o el servidor está desconectado.	Comprueba que el servidor se está ejecutando. Comprueba la configuración de NAT.
0x85002004	E_FAIL_ABORT	Este error se usa para interrumpir hanging sync y no se mostrará a los usuarios. Se mostrará en los datos de diagnóstico si fuerzas una sincronización interactiva, eliminas la cuenta o actualizas su configuración.	Nada

CÓDIGO HEXADECIMAL	ASIGNACIÓN	MENSAJE DESCRIPTIVO	ACCIONES QUE DEBE REALIZAR EL ADMINISTRADOR
0x85010017	E_HTTP_SERVICE_UNAVAIL	No se puede conectar al servidor en este momento. Espera un momento o verifica la configuración de la cuenta.	Comprueba el nombre del servidor para asegurarse de que es correcto. Espera a que el servidor vuelva a estar conectado. Si el problema persiste, vuelve a aprovisionar la cuenta.
0x86000C0D	E_NEXUS_STATUS_MAILBOX_SERVEROFFLINE	No se puede conectar al servidor en este momento. Espera un momento o verifica la configuración de la cuenta.	Comprueba el nombre del servidor para asegurarse de que es correcto. Espera a que el servidor vuelva a estar conectado. Si el problema persiste, vuelve a aprovisionar la cuenta.
0x85030027	E_ACTIVESYNC_GETCERT	El servidor Exchange requiere un certificado.	Importar el certificado EAS apropiado en el Surface Hub.
0x86000C2B	E_NEXUS_STATUS_INVALID_POLICYKEY	La cuenta está configurada con directivas que no son compatibles con Surface Hub.	Deshabilitar la directiva PasswordEnabled para esta cuenta. Se ha producido un error que se producía un error en la política si la cuenta no recibe notificaciones del servidor en el intervalo de actualización de la Directiva.
0x85010005	E_HTTP_NOT_FOUND	El nombre del servidor no es válido.	Comprueba el nombre del servidor para asegurarse de que es correcto. Si el problema persiste, vuelve a aprovisionar la cuenta.
0x85010014	E_HTTP_SERVER_ERROR	No se puede conectar al servidor.	Comprueba el nombre del servidor para asegurarse de que es correcto. Desencadena una sincronización y, si el problema persiste, vuelve a aprovisionar la cuenta.

CÓDIGO HEXADECIMAL	ASIGNACIÓN	MENSAJE DESCRIPTIVO	ACCIONES QUE DEBE REALIZAR EL ADMINISTRADOR
0x80072EE7	WININET_E_NAME_NOT_RESOLVED	No se pudo resolver el nombre del servidor o la dirección.	Asegúrate de que el nombre del servidor está escrito correctamente.
0x8007052F	ERROR_ACCOUNT_RESTRICTION	Durante la detección automática del servidor Exchange, se aplica una directiva que impide que el usuario que haya iniciado sesión inicie sesión en el servidor.	Se trata de un problema de temporización. Vuelve a comprobar las credenciales de cuenta. Intenta volver a aprovisionarlas cuando sean correctas.
0x800C0019	INET_E_INVALID_CERTIFICATE	El certificado de seguridad necesario para acceder a este recurso no es válido.	Instala el certificado correcto de ActiveSync necesario para la cuenta del dispositivo proporcionada.
0x80072F0D	WININET_E_INVALID_CA	La entidad de certificación no es válida o es incorrecta. No se pudo detectar automáticamente el servidor Exchange porque falta un certificado.	Instala el certificado correcto de ActiveSync necesario para la cuenta del dispositivo proporcionada.
0x80004005	E_FAIL	No se encontró el dominio proporcionado. El servidor Exchange no se pudo detectar automáticamente y no se proporcionó en la configuración.	Asegúrate de que el dominio especificado es el FQDN y de que se ha especificado un servidor Exchange en el cuadro de texto del servidor Exchange.

Ponerse en contacto con soporte técnico

Si tiene alguna pregunta o necesita ayuda, puede crear una solicitud de soporte técnico.

Contenidos relacionados

- Solucionar problemas de conexión de Miracast a Surface Hub

Problemas conocidos: Surface Hub

12/01/2022 • 4 minutes to read

En este artículo se enumeran los problemas conocidos para Surface Hubs que ejecutan el sistema operativo actual, Windows 10 Team 2020 Update.

Para asegurarse de Surface Hub recibe las actualizaciones más recientes, **** inicie sesión con una cuenta de administrador y seleccione Todas las aplicaciones Configuración Actualización y seguridad Windows Actualización y, a continuación, instale todas las > **** > **** > **** actualizaciones.

PROBLEMA	DESCRIPCIÓN	SOLUCIÓN
Al usar la aplicación pizarra en Surface Hub dispositivos, el contenido no se puede compartir por correo electrónico.	Al pasar por el flujo de exportación de pizarra para enviar por correo electrónico el contenido de la aplicación pizarra, Surface Hub dispositivos están mostrando actualmente "El dispositivo no está configurado para correo electrónico". Como resultado, el contenido de la pizarra no se puede compartir por correo electrónico.	Microsoft conoce y está investigando activamente este problema. Microsoft proporcionará información adicional sobre una resolución lo antes posible.
Algunos Surface Hubs están experimentando problemas de conectividad con sus áreas de trabajo de Azure Log Analytics (anteriormente conocidas como OMS).	Para los dispositivos Surface Hub afectados, al usar Azure Monitor, no se notifica ningún dato al área de trabajo.	Microsoft conoce y está investigando activamente este problema. Microsoft proporcionará información adicional sobre una resolución lo antes posible.
Algunos Surface Hubs se reinician cuando un usuario selecciona "Finalizar sesión".	Cuando Surface Hub usuarios del dispositivo seleccionan la funcionalidad "Finalizar sesión" para borrar los datos de usuario, el dispositivo Surface Hub puede detectar erróneamente un error de limpieza, lo que obliga a reiniciar Windows para garantizar que la limpieza se realiza correctamente.	Microsoft conoce y está investigando activamente este problema. Microsoft proporcionará información adicional sobre una resolución lo antes posible.
Algunos Surface Hubs pueden dejar de sincronizar el reloj de su equipo con time.windows.com si han estado afiliados a Azure Active Directory o configurados sin ninguna filiación. Cuando esta sincronización no funciona, el tiempo en el dispositivo puede desviar de la hora real.	La desviación del reloj más allá de 5 minutos puede provocar errores de autenticación en escenarios Surface Hub estándar, incluido Teams inicio de sesión.	En el dispositivo afectado, ve a **Todas**las aplicaciones Configuración Hora & idioma Fecha & hora y desactiva Establecer hora automáticamente y vuelve > **** > **a** > **** activar. **** Microsoft también está investigando activamente este problema y proporcionará información adicional sobre una resolución lo antes posible.
La configuración de calidad de servicio (QoS) no funciona como se esperaba	Después de configurar la configuración de QoS a través de la directiva MDM o el paquete de aprovisionamiento, las marcas DSCP no se aplican al tráfico multimedia Teams o Skype Empresarial (SfB).	Microsoft conoce y está investigando activamente este problema. Microsoft proporcionará información adicional sobre una resolución lo antes posible.

PROBLEMA	DESCRIPCIÓN	SOLUCIÓN
Se produce un error en la sincronización de calendario de cuentas de dispositivo híbrida con buzones locales.	Surface Hub dispositivos usan de forma predeterminada la autenticación moderna para cuentas que existen en Azure AD, incluso si tienen buzones locales que no funcionan con esta característica. En este escenario, Exchange deja de sincronizar reuniones con el dispositivo. Como resultado, el dispositivo no recibe ni muestra nuevas reuniones.	Después de instalar KB4598291 (o un Windows CU posterior), el CSP de SurfaceHub tiene un nuevo parámetro ExchangeModernAuthEnabled disponible para alternar el uso de la autenticación moderna. Esto se puede establecer en false a través de la directiva MDM o el paquete de aprovisionamiento para evitar que el concentrador use la autenticación moderna.
Un pequeño subconjunto de dispositivos Surface Hub v1 no pueden actualizar automáticamente a la actualización Windows 10 Team 2020.	Este pequeño subconjunto de dispositivos Surface Hub v1 están en un estado que impide la compatibilidad con la actualización directa a través de Windows Update.	Vuelva a crear manualmente la imagen del dispositivo en la Windows 10 Team 2020 Update con la herramienta Surface Hub recuperación.
Surface Hub muestra el mensaje "Ningún dispositivo de arranque" después de intentar instalar la actualización Windows 10 Team 2020.	Durante el Windows update para Windows 10 Team 2020, algunos dispositivos Hub v1 pasarán a un estado no arrancable.	Vuelva a crear manualmente la imagen del dispositivo en la Windows 10 Team 2020 Update con la herramienta Surface Hub recuperación.
Los dispositivos hub 2S no pueden recibir actualizaciones de controladores con WSUS.	Surface Hub 2S admite Windows Update y Windows Update para empresas para distribuir controladores; no se admite Windows Server Update Services (WSUS).	Si usa WSUS, migre a Windows Update for Business. **Más información:** ¿Qué es Windows actualización para empresas?
El Centro de acciones tiene un vínculo de Configuración no se puede hacer clic.	Este vínculo no debe aparecer en Windows 10 Team y puede causar confusión.	La funcionalidad es la misma que antes de la actualización de 2020; la sección Aplicaciones de la menú Inicio debe usarse para iniciar la Configuración aplicación.

Resumen

12/01/2022 • 2 minutes to read

En este artículo se describe cómo usar la función de recuperación en la nube si BitLocker te pide inesperadamente en un Surface Hub dispositivo.

> **NOTE**
> Solo debes seguir estos pasos si una clave de recuperación de BitLocker no está disponible.

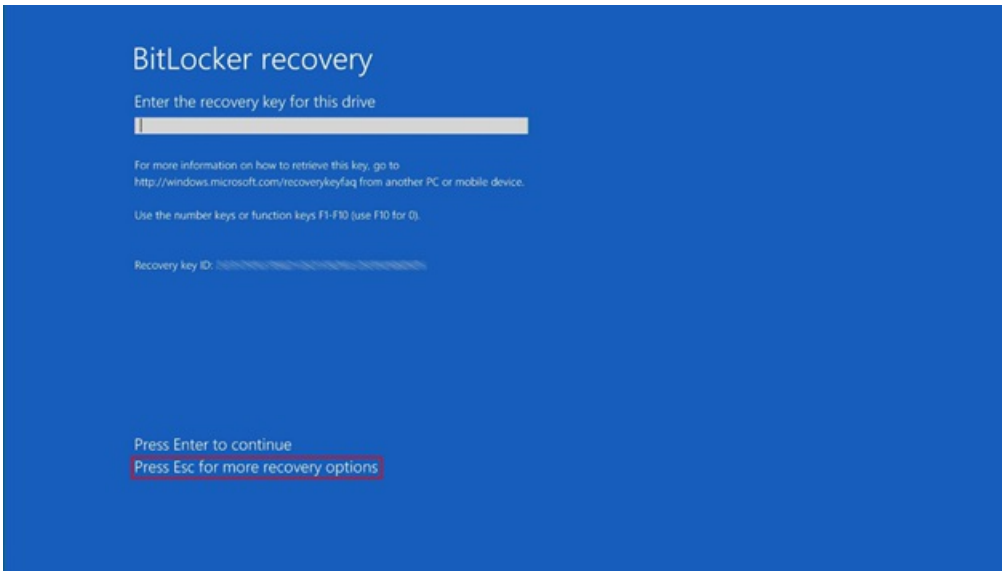
> **WARNING**
> - Este proceso de recuperación elimina el contenido de la unidad interna. Si se produce un error en el proceso, la unidad interna se volverá completamente inutilizable. Si esto ocurre, tendrá que registrar una solicitud de servicio con Microsoft para obtener una resolución.
> - Una vez completado el proceso de recuperación, el dispositivo se restablecerá a la configuración de fábrica y se devolverá a su estado de experiencia fuera de la caja.
> - Después de la recuperación, Surface Hub debe volver a configurarse completamente.

> **IMPORTANT**
> Este proceso requiere una conexión a Internet abierta que no use un proxy u otro método de autenticación.

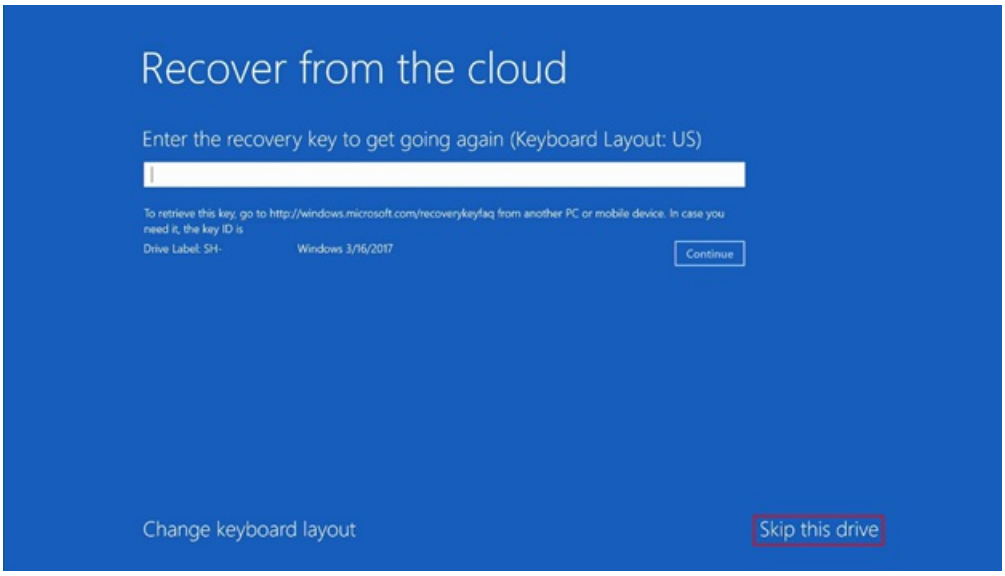
Proceso de recuperación en la nube

Para realizar una recuperación en la nube, siga estos pasos:

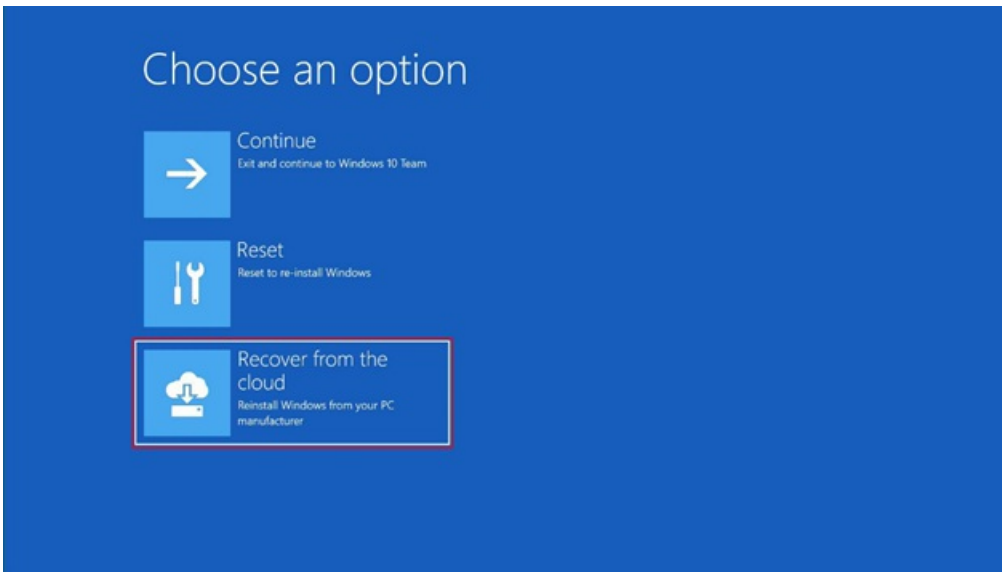
1. Seleccione **Presionar Esc para obtener más opciones de recuperación.**



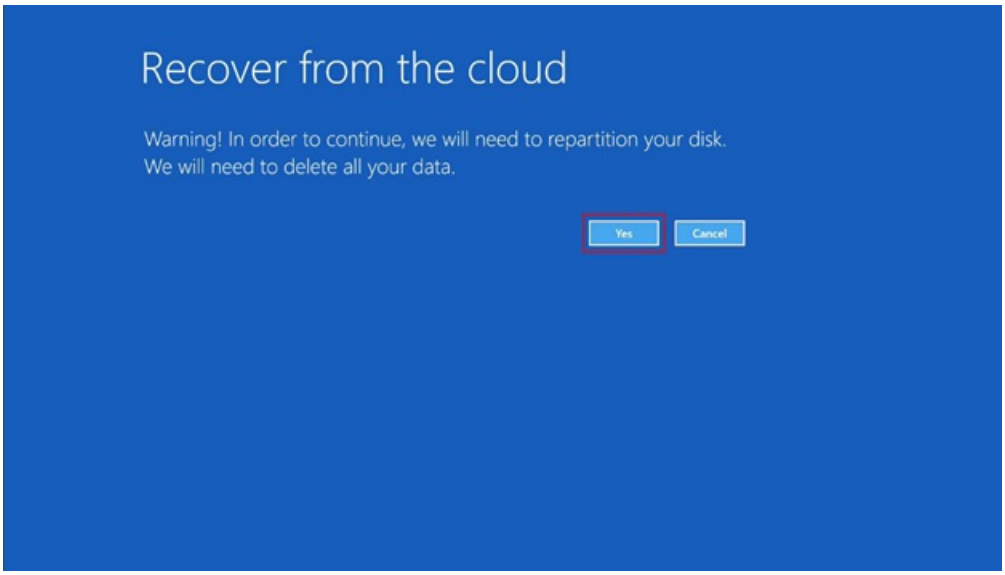
2. Seleccione **Omitir esta unidad**.



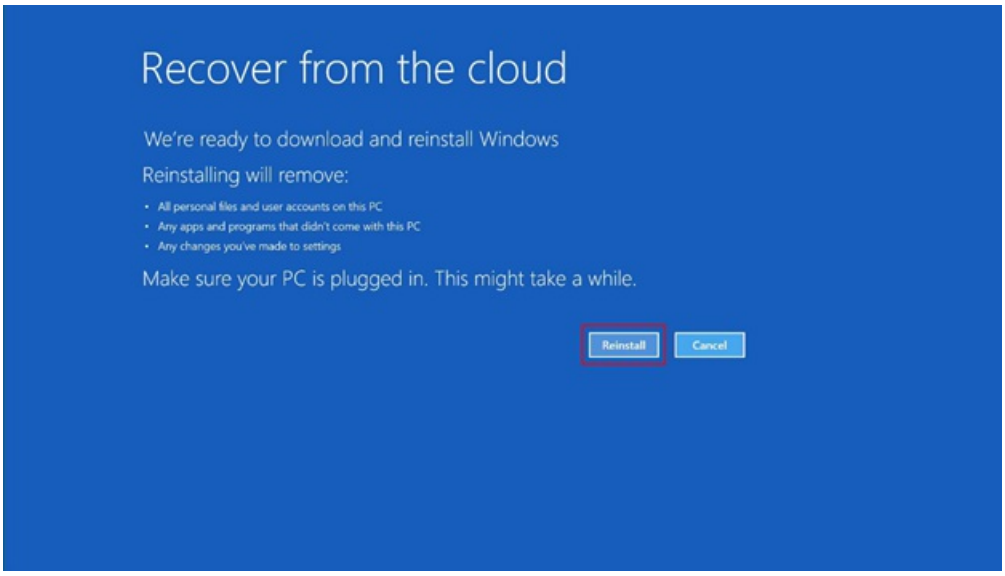
3. Seleccione **Recuperar desde la nube**.

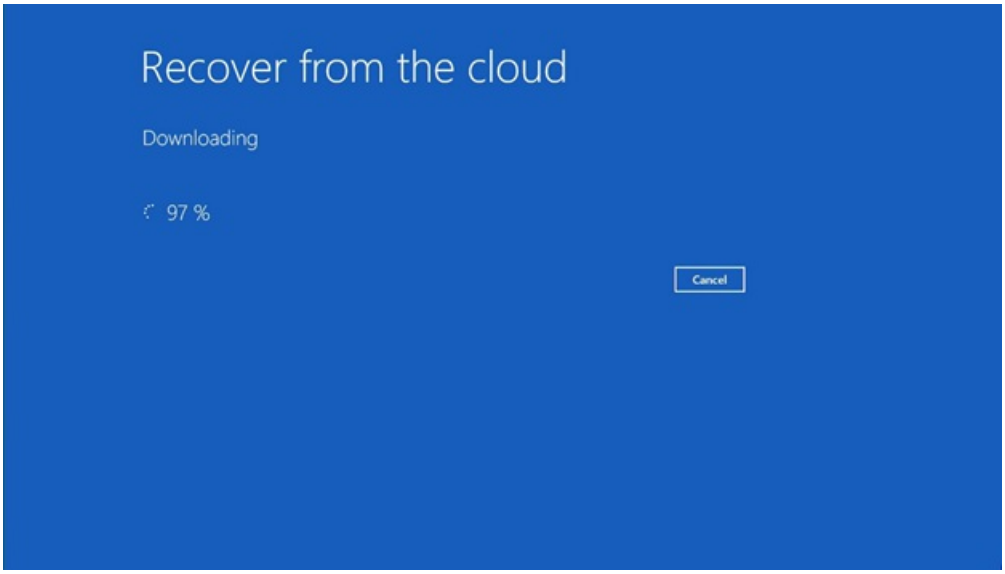


4. Seleccione **Sí**.

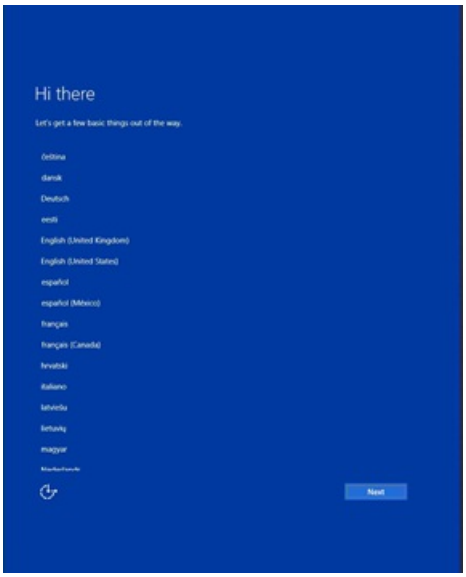


5. Seleccione **Reinstalar**.





6. Una vez completado el proceso de recuperación en la nube, inicie la reconfiguración mediante **la experiencia de inicio de la caja**.

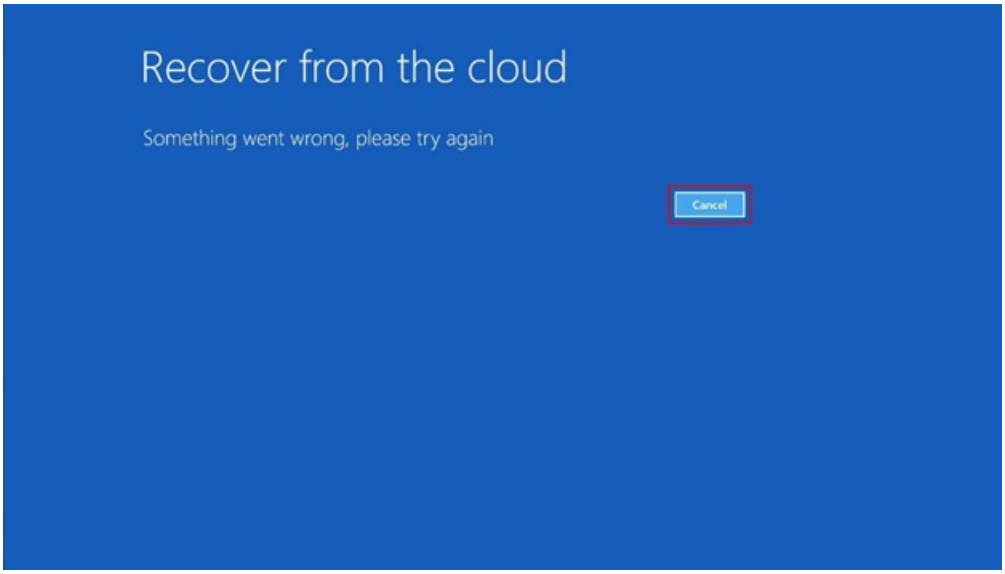


Mensaje de error "Algo salió mal"

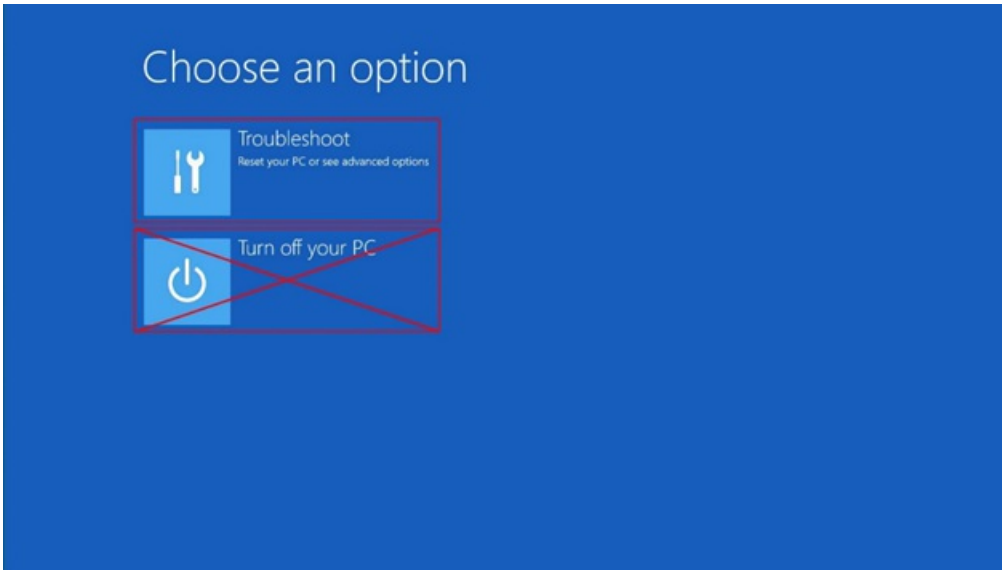
Este error suele deberse a problemas de red que se producen durante la descarga de recuperación. Cuando se produzca este problema, no desactive el concentrador porque no podrá reiniciarlo. Si recibe este mensaje de

error, vuelva al paso "Recuperar de la nube" y, a continuación, reinicie el proceso de recuperación.

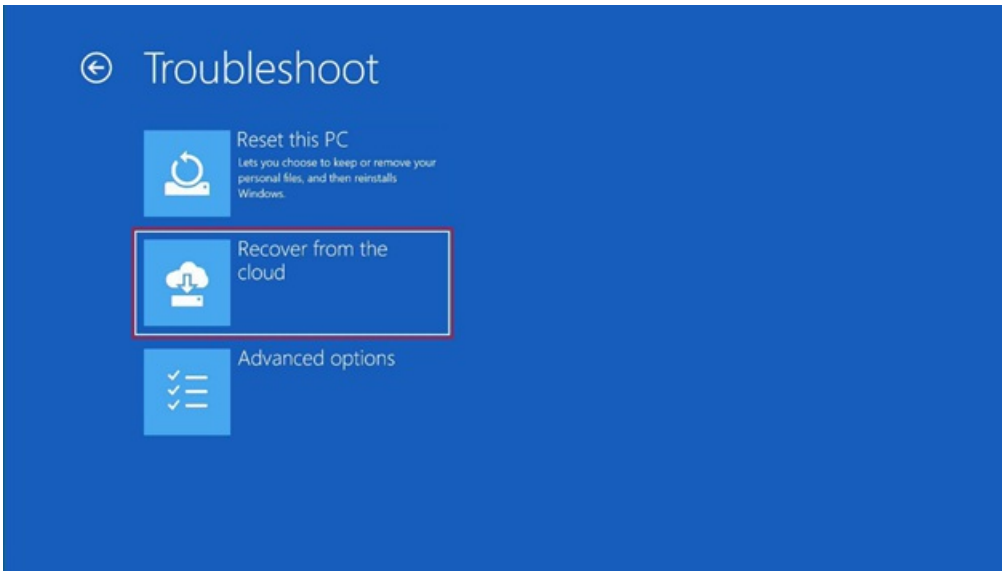
1. Seleccione **Cancelar**.



2. Seleccione **Solucionar problemas**.

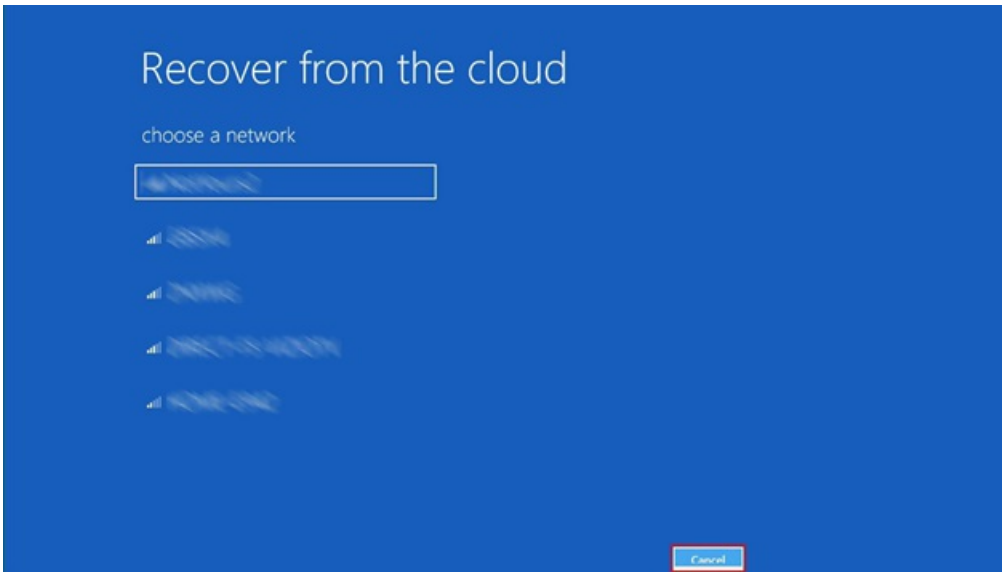


3. Seleccione **Recuperar desde la nube**.



4. Si no **se encuentra** un error en la red cableada, seleccione **Cancelar**y, a continuación, deje que el

Surface Hub detección de la red cableada.



Uso de la herramienta de diagnóstico de hardware de Surface Hub para probar una cuenta del dispositivo

12/01/2022 • 4 minutes to read

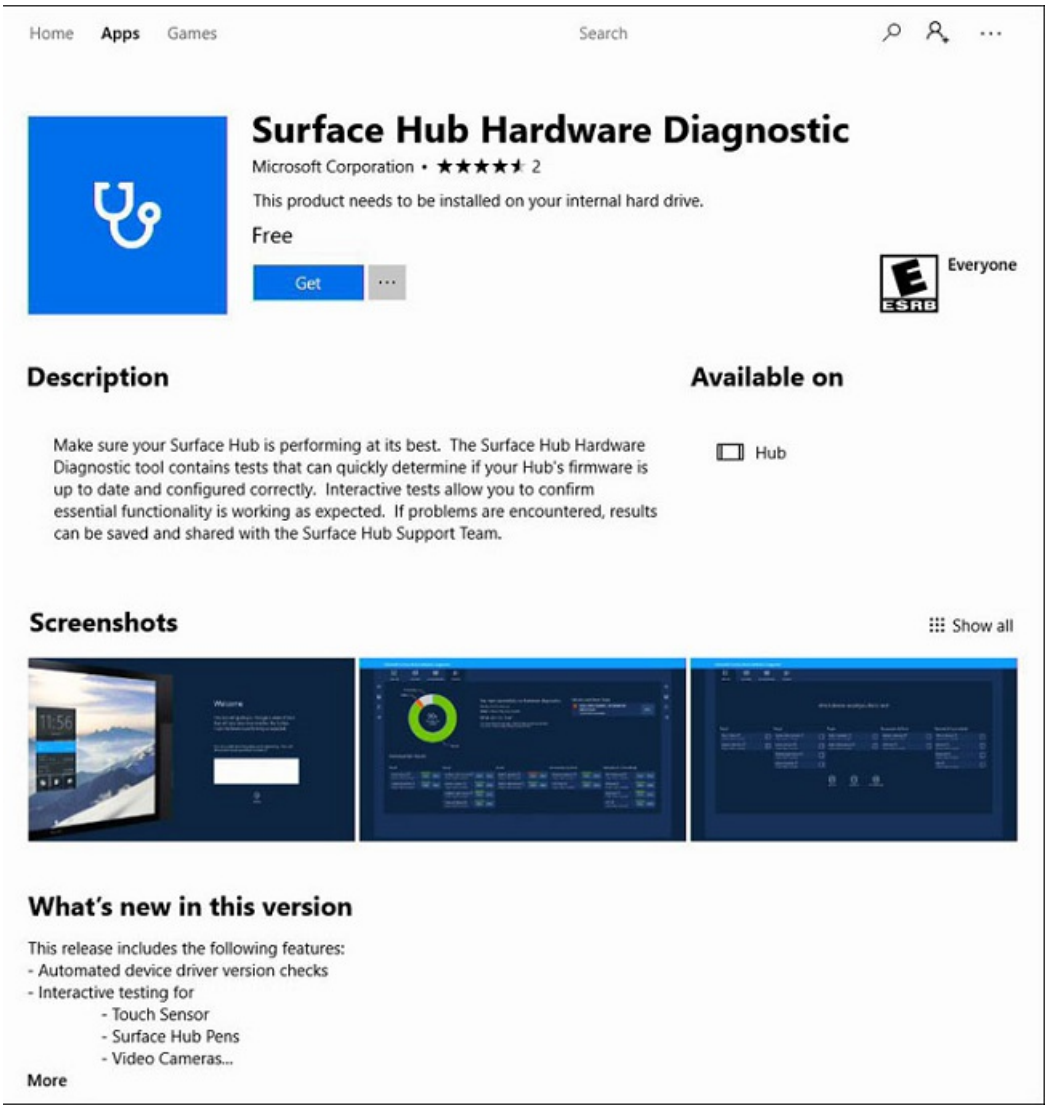
Introducción

> **NOTE**
> La sección "Account Configuración" de la Surface Hub de diagnóstico de hardware no recopila ninguna información. El correo electrónico y la contraseña que se introducen como entrada solo se usan directamente en el entorno y no se recopilan ni transfieren a nadie. La información de inicio de sesión solo persiste hasta que la aplicación se cierra o finaliza la sesión actual en el Surface Hub.

> **IMPORTANT**
> - Los privilegios de administrador no son necesarios para ejecutar esta aplicación.
> - Los resultados del diagnóstico deben analizarse con el administrador local antes de abrir una llamada de servicio con Microsoft.

Surface Hub Diagnóstico de hardware

De forma predeterminada, la Surface Hub de diagnóstico de hardware no está instalada en versiones anteriores del sistema Surface Hub hardware. La aplicación está disponible de forma gratuita desde el Microsoft Store. Los privilegios de administrador son necesarios para instalar la aplicación.



Acerca de la Surface Hub de diagnóstico de hardware

La Surface Hub de diagnóstico de hardware es una herramienta fácil de navegar que permite al usuario probar muchos de los componentes de hardware dentro del Surface Hub dispositivo. Esta herramienta también puede probar y comprobar una cuenta Surface Hub dispositivo. En este artículo se describe cómo usar la prueba account Configuración dentro de la Surface Hub de diagnóstico de hardware.

> **NOTE**
> La cuenta del dispositivo para el Surface Hub debe crearse antes de realizar cualquier prueba. La guía Surface Hub administrador proporciona instrucciones y scripts de PowerShell para ayudarle a crear cuentas de dispositivos locales, en línea (Office365) o híbridas. Para obtener más información, vaya al tema Crear y probar una cuenta de dispositivo (Surface Hub) de la guía.

Proceso de prueba de cuenta de dispositivo

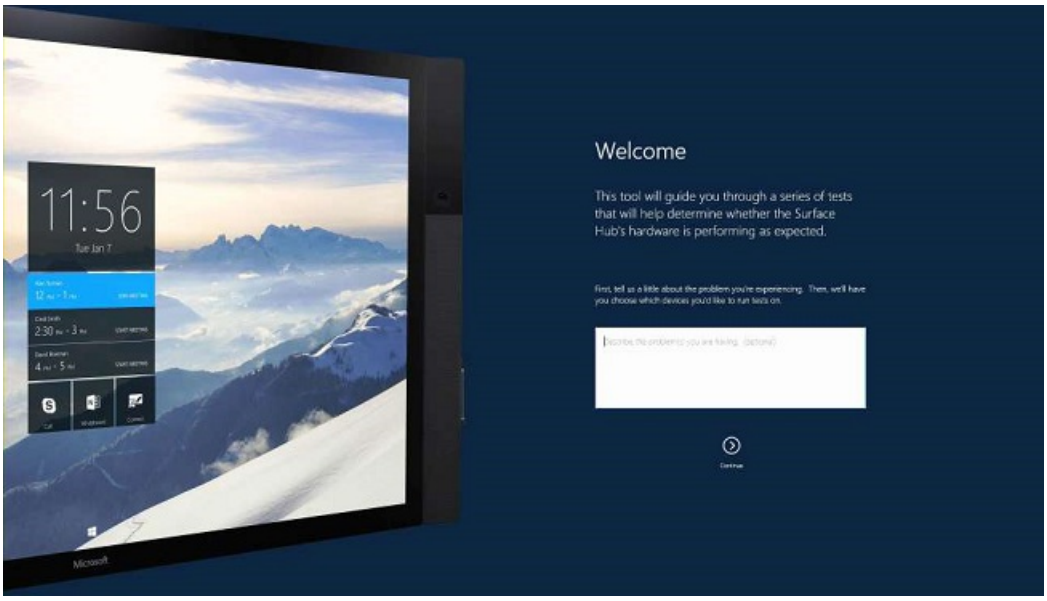
1. Vaya a **Todas las aplicaciones**y, a continuación, busque la Surface Hub de diagnóstico de hardware.

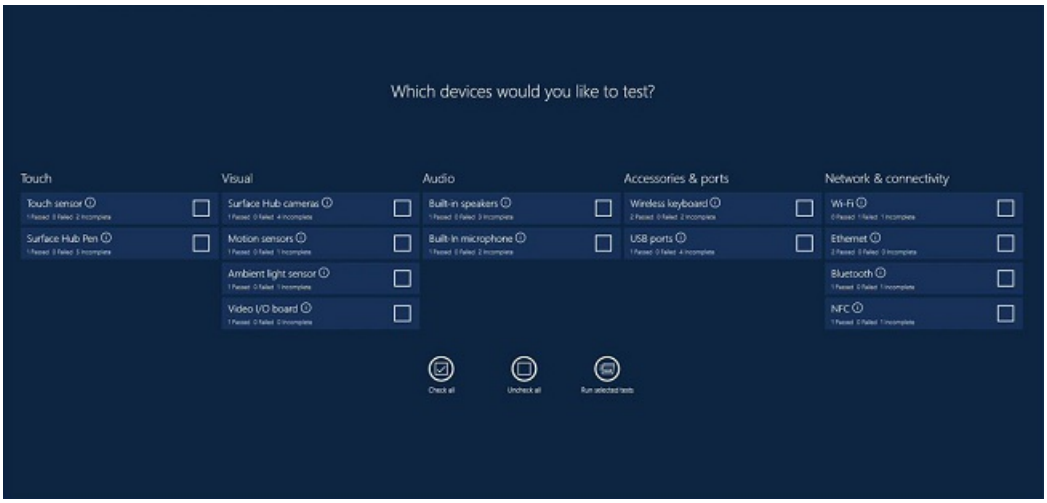
2. Cuando se inicia la aplicación, la **página de** bienvenida proporciona una ventana de texto para documentar el motivo por el que está probando el concentrador. Esta nota se puede guardar en USB junto con los resultados de diagnóstico al finalizar las pruebas. Una vez que termine de escribir una nota, seleccione el **botón** Continuar.

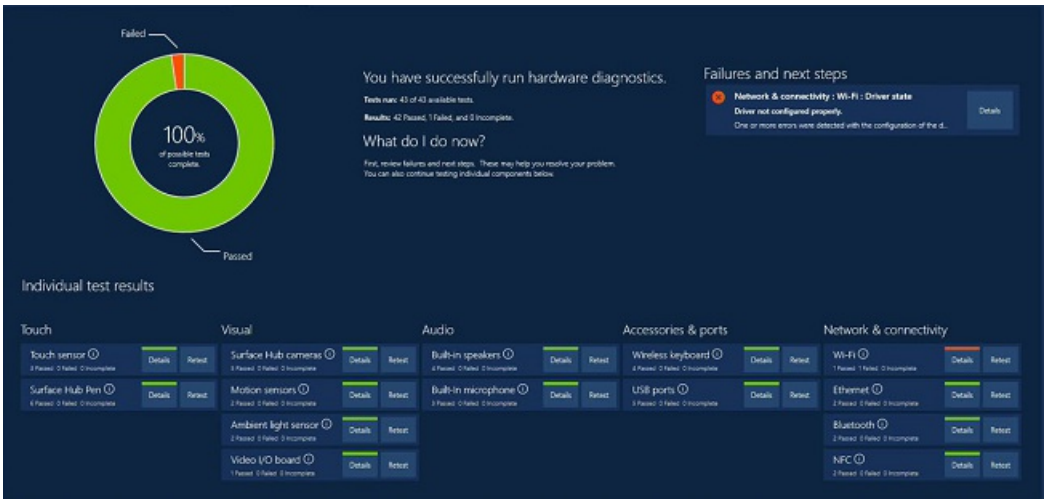
NOTE

Al guardar los resultados de diagnóstico, no cambie la ruta de acceso predeterminada ni seleccione un subdirectorio. Los archivos se pueden copiar más adelante a través de la aplicación Explorador de archivos.

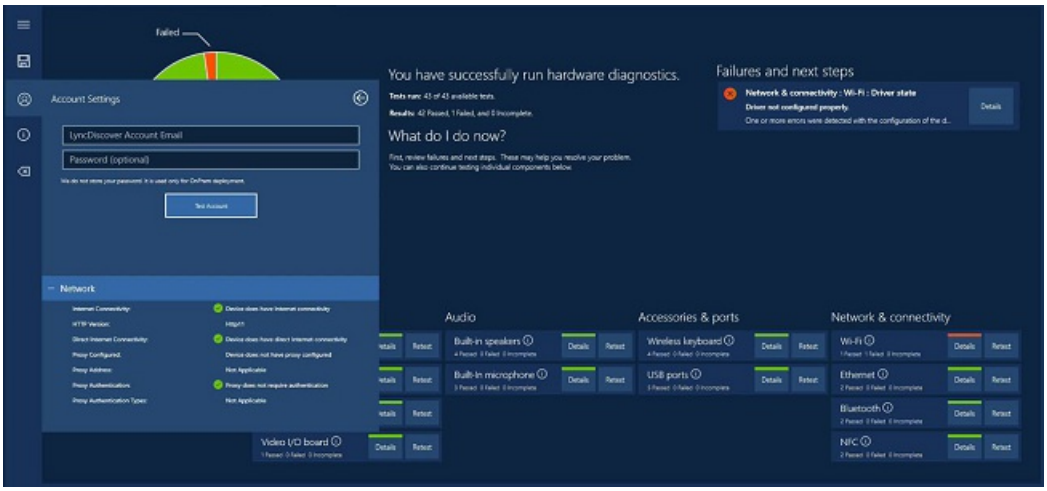


3. La siguiente pantalla le ofrece la opción de probar todos o algunos de los Surface Hub componentes. Para empezar a probar la cuenta del dispositivo, selecciona el icono **Resultados de** la prueba.

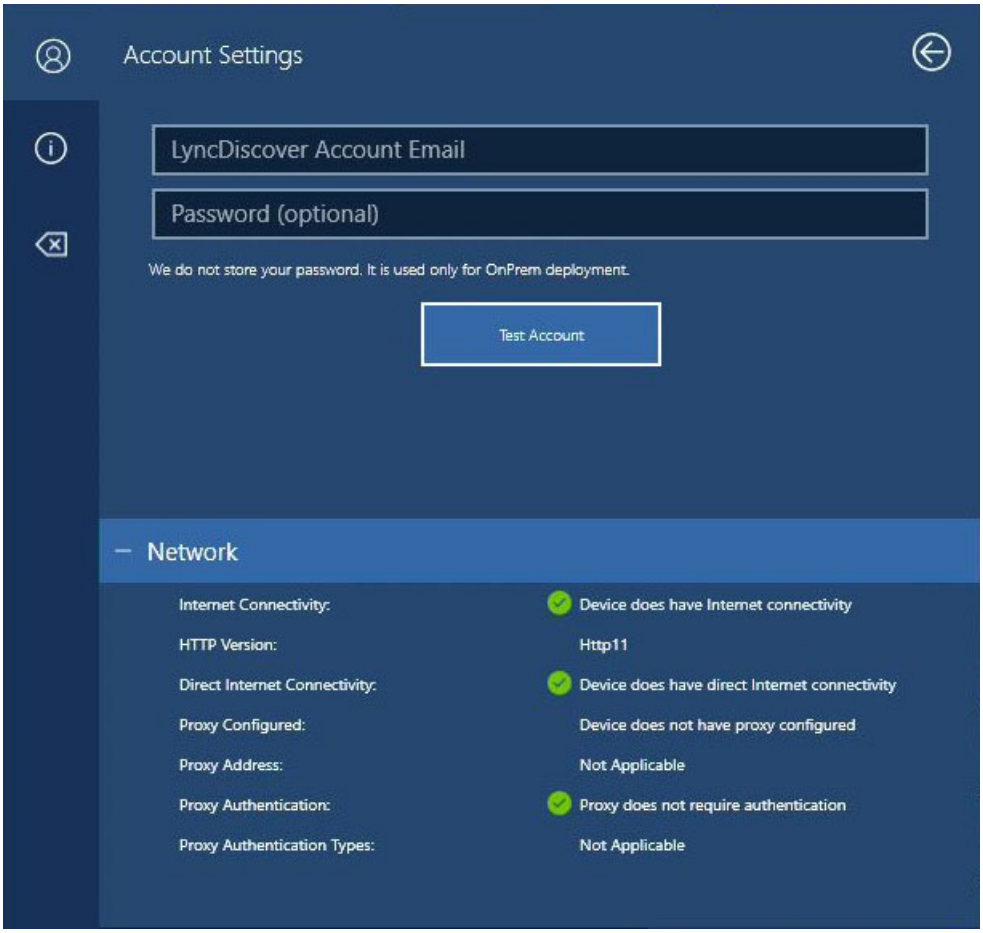




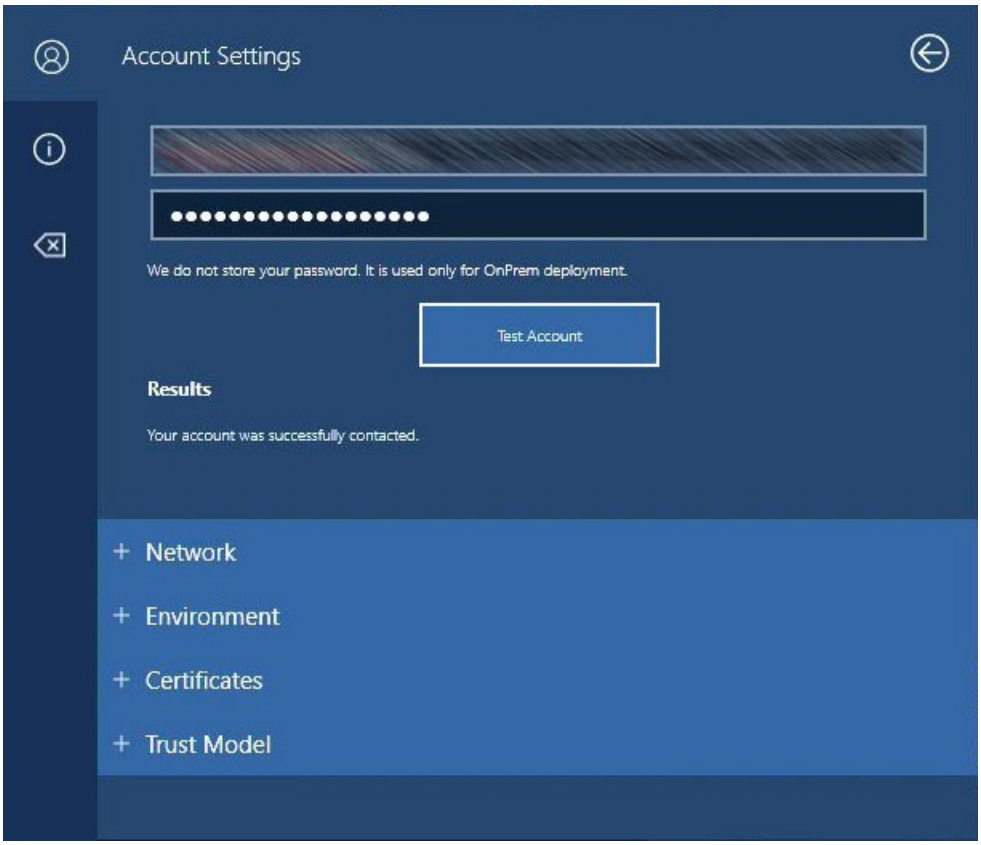
4. Seleccione **Cuenta Configuración**.



La pantalla Configuración cuenta se usa para probar la cuenta del dispositivo.

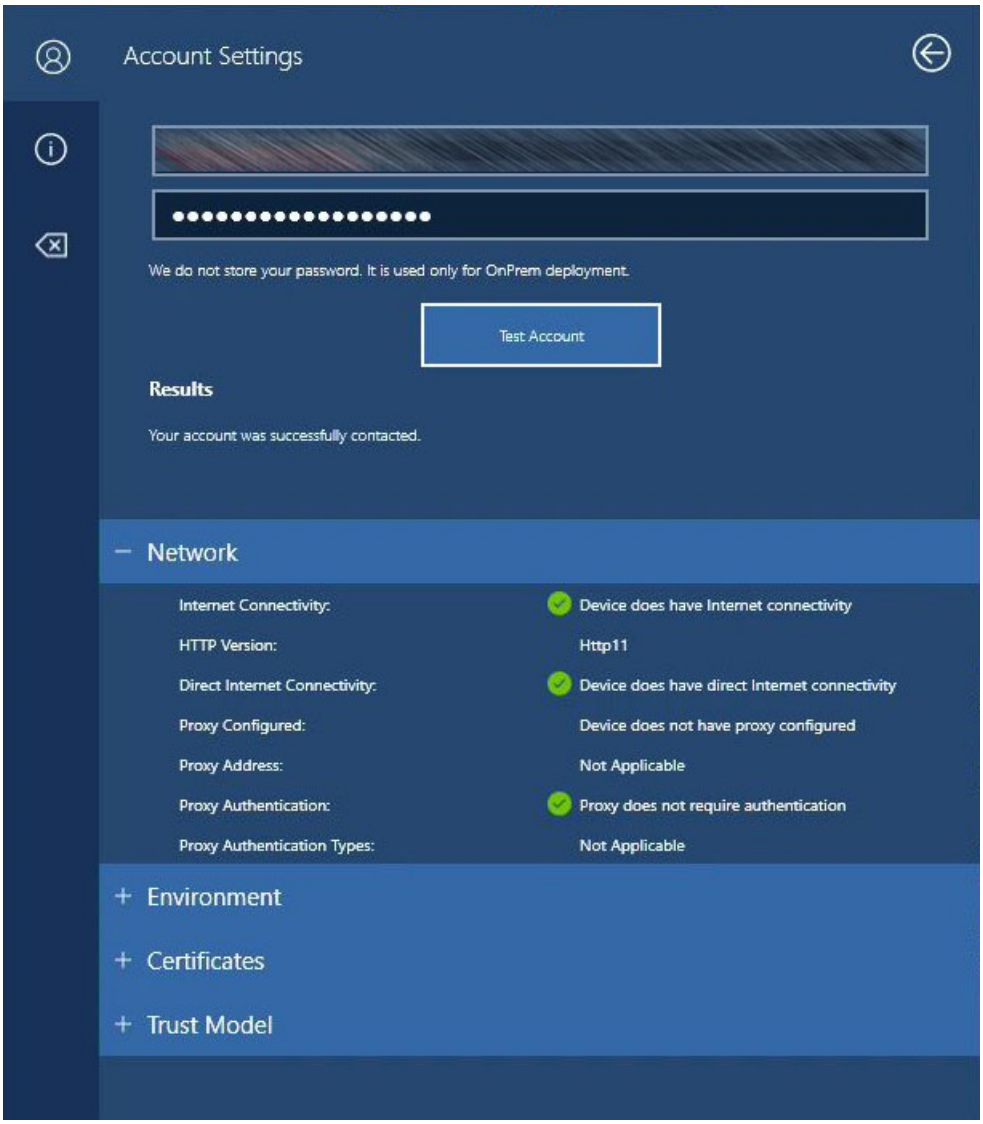


5. Escribe la dirección de correo electrónico de tu cuenta de dispositivo. La contraseña es opcional, pero se recomienda. Seleccione el **botón Probar cuenta** cuando esté listo para continuar.

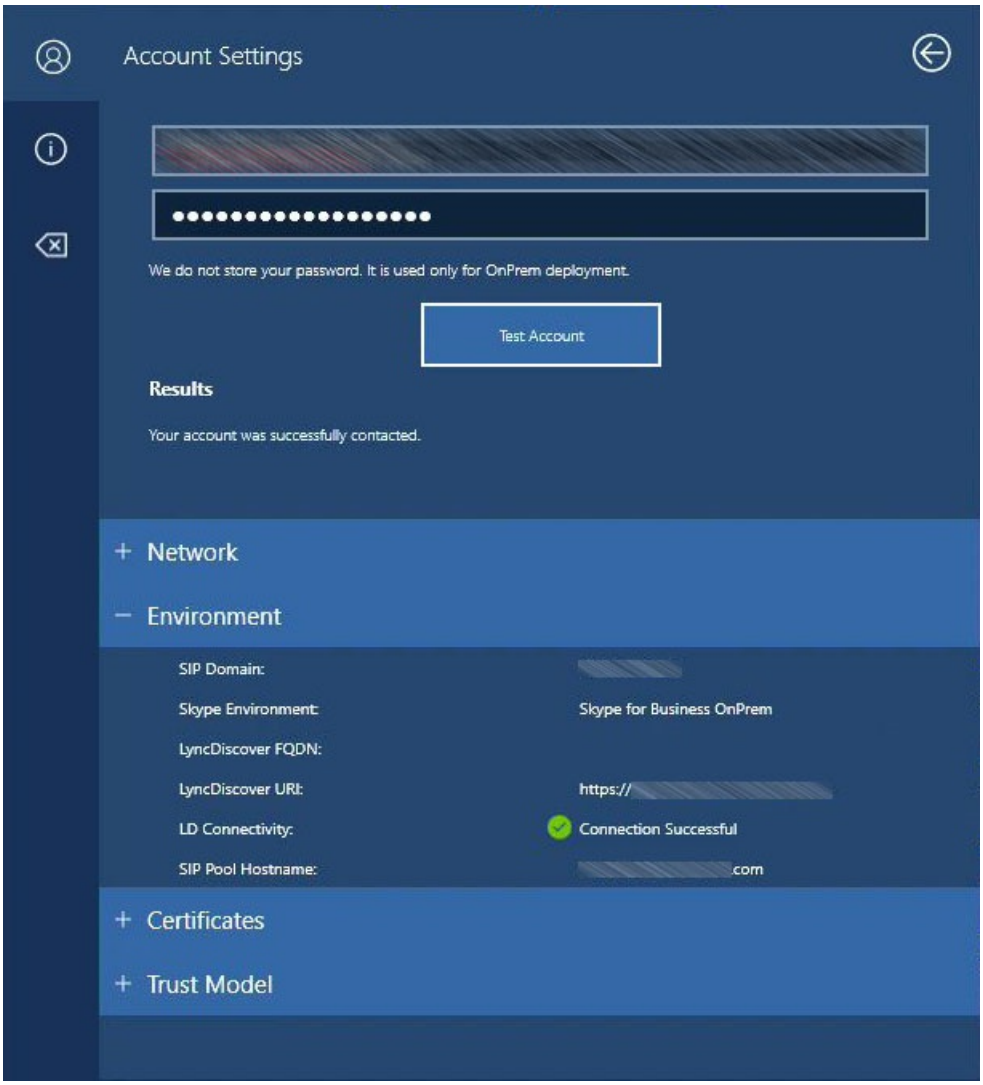


6. Una vez finalizadas las pruebas, revise los resultados de las cuatro áreas de prueba. Cada sección se puede expandir o contraer seleccionando el signo Más o Menos junto a cada tema.

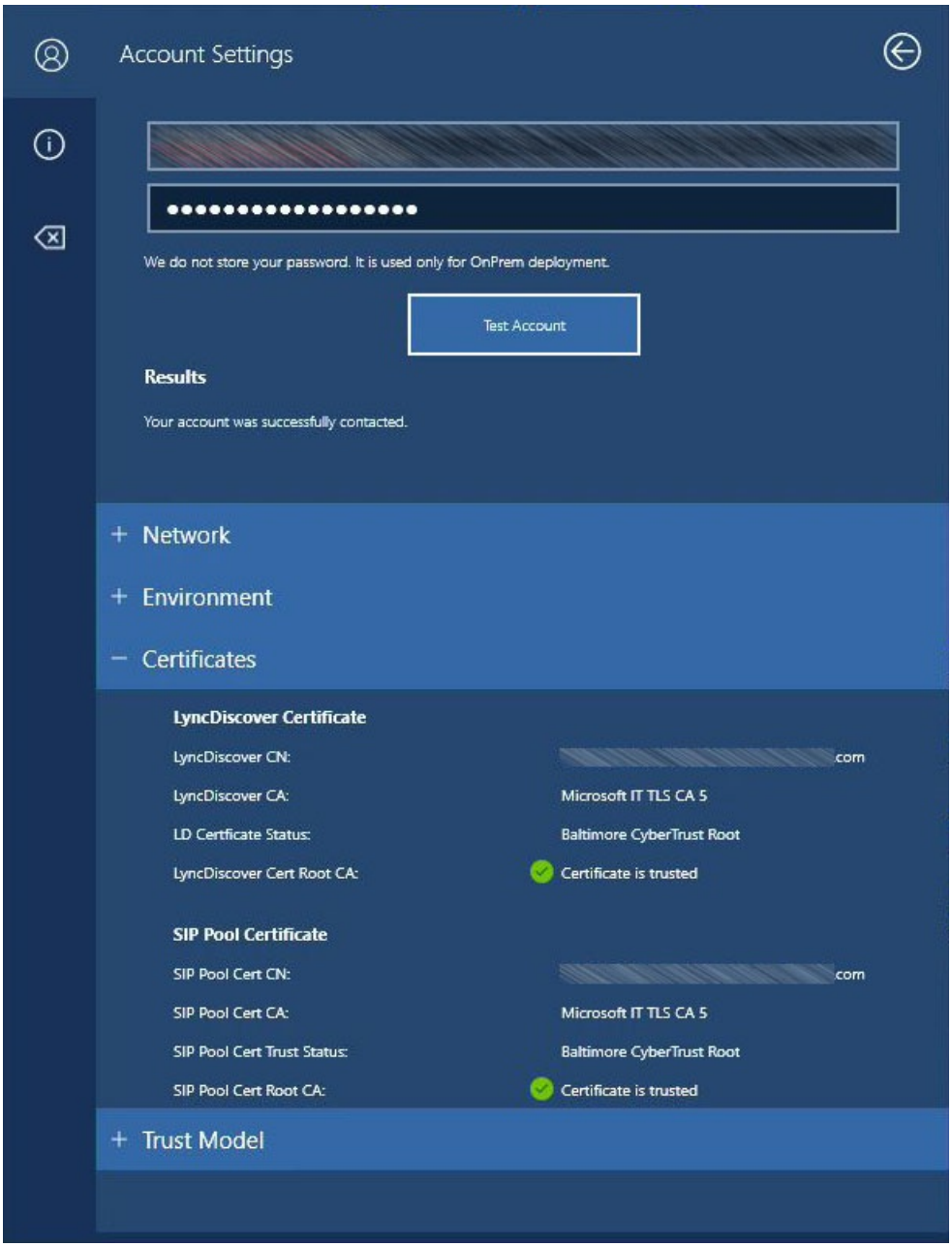
   Red


Account Settings
We do not store your password. It is used only for OnPrem deployment.
Test Account
Results
Your account was successfully contacted.
Network
Internet Connectivity:
Device does have Internet connectivity
HTTP Version:
Http11
Direct Internet Connectivity:
Device does have direct Internet connectivity
Proxy Configured:
Device does not have proxy configured
Proxy Address:
Not Applicable
Proxy Authentication:
Proxy does not require authentication
Proxy Authentication Types:
Not Applicable
Environment
Certificates
Trust Model

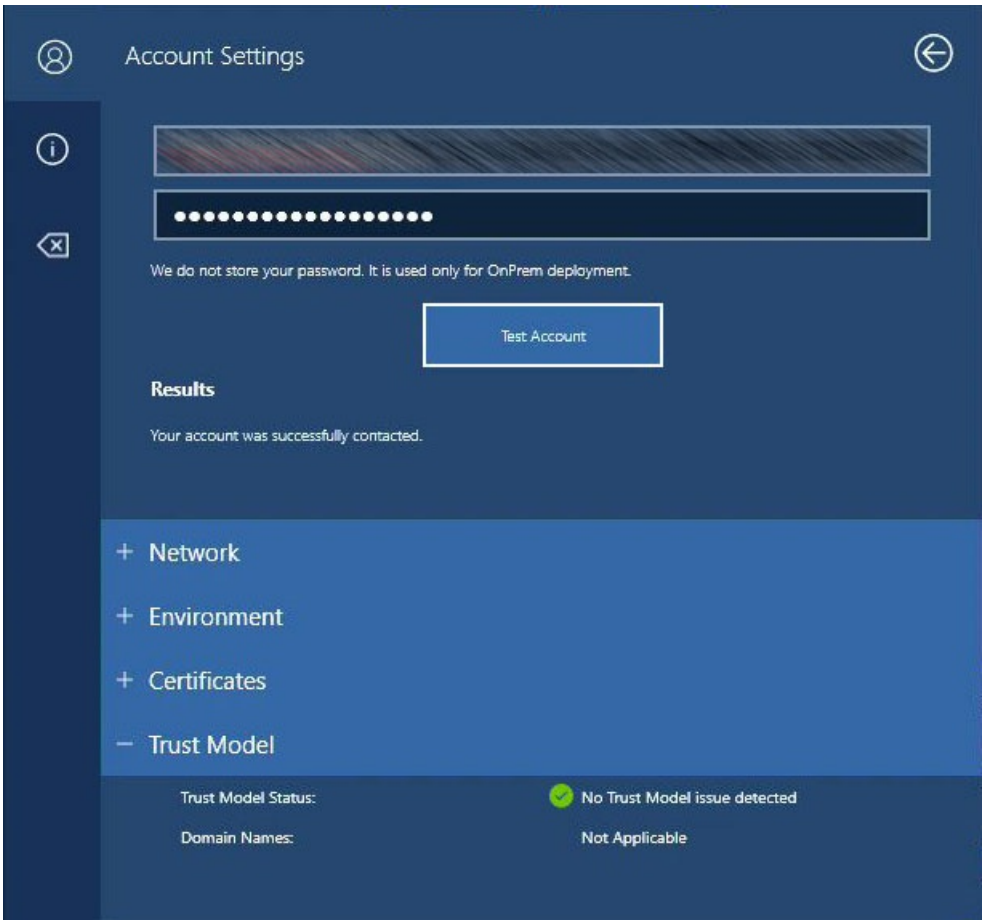
Entorno



Certificados



Modelo de confianza



Apéndice

Mensajes de campo y resolución

Red

CAMPO	CORRECTO	ERROR	COMENTARIO	REFERENCIA
Conectividad a Internet	El dispositivo tiene conectividad a Internet	El dispositivo no tiene conectividad a Internet	Comprueba la conectividad a Internet, incluida la conexión proxy	
Versión HTTP	1.1	1.0	Si se encuentra HTTP 1.0, provocará problemas con WU y Store	
Conectividad directa a Internet	El dispositivo tiene un dispositivo configurado por proxy que no tiene ningún proxy configurado	N/A	Informativo. ¿Está el dispositivo detrás de un proxy?	
Dirección proxy			Si está configurado, devuelve la dirección proxy.	

CAMPO	CORRECTO	ERROR	COMENTARIO	REFERENCIA
Autenticación de proxy	El proxy no requiere autenticación	Proxy requiere autenticación de proxy	El resultado puede ser un falso positivo si un usuario ya tiene una sesión abierta en Edge y se ha autenticado a través del proxy.	
Tipos de autenticación de proxy			Si se usa la autenticación de proxy, devuelve los métodos de autenticación anunciados por el proxy.	

Entorno

CAMPO	CORRECTO	ERROR	COMENTARIO	REFERENCIA
Dominio SIP			Informativo.	
Skype Entorno	Skype Empresarial Online, Skype Empresarial OnPrem, Skype Empresarial Hybrid	Informativo.	Qué tipo de entorno se detectó. Nota: El híbrido solo se puede detectar si se introduce la contraseña.	
LyncDiscover FQDN			Informativo. Muestra el resultado dns de LyncDiscover	
LyncDiscover URI			Informativo. Muestra la dirección URL usada para realizar una LyncDiscover en el entorno.	
LyncDiscover	Conexión correcta	Error en la conexión	Respuesta del servicio web LyncDiscover.	
Nombre de host del grupo SIP			Informativo. Mostrar el nombre del grupo SIP detectado en LyncDiscover	

Certificados (solo híbridos locales)

Certificado de LyncDiscover

CAMPO	CORRECTO	ERROR	COMENTARIO	REFERENCIA
LyncDiscover Cert CN			Informativo. Muestra el certificado LD Nombre común	

CAMPO	CORRECTO	ERROR	COMENTARIO	REFERENCIA
LyncDiscover Cert CA			Informativo. Muestra la CA de certificado DE LD	
LyncDiscover Cert Root CA			Informativo. Muestra la CA raíz de certificado de LD, si está disponible.	
Estado de confianza ld	El certificado es de confianza.	El certificado no es de confianza, agregue la CA raíz.	Compruebe el certificado en el almacén de certificados local. Devuelve positivo si la máquina confía en el certificado.	Descargar e implementar Skype Empresarial certificados con PowerShell / Elementos admitidos para Surface Hub paquetes de aprovisionamiento

Certificación de grupo SIP

CAMPO	CORRECTO	ERROR	COMENTARIO	REFERENCIA
CERT DE GRUPO SIP			(CONTENTS)	
CA de certificado de grupo SIP			(CONTENTS)	
Estado de confianza del grupo SIP	El certificado es de confianza.	El certificado no es de confianza, agregue la CA raíz.	Compruebe el certificado en el almacén de certificados local y devuelva un positivo si los dispositivos confían en el certificado.	
CA raíz de certificado de grupo SIP			Información. Mostrar la CA raíz de certificado de grupo SIP, si está disponible.	

Modelo de confianza (solo híbrido local)

CAMPO	CORRECTO	ERROR	COMENTARIO	REFERENCIA
Estado del modelo de confianza	No se detectó ningún problema del modelo de confianza.	Dominio SIP y dominio de servidor son diferentes, agregue los siguientes dominios.	Compruebe el fqdn ld/ nombre del servidor LD/ nombre del servidor de grupo de servidores para el problema del modelo de confianza.	

CAMPO	CORRECTO	ERROR	COMENTARIO	REFERENCIA
Nombres de dominio			Devuelve la lista de dominios que se deben agregar para que SFB se conecte.	

Soluciona problemas de Miracast en Surface Hub

12/01/2022 • 6 minutes to read

Surface Hub admite la proyección inalámbrica a través del protocolo Miracast. La mayoría de los monitores y adaptadores inalámbricos disponibles hoy en día usan la implementación original de Miracast. Surface Hub usa una versión de Miracast ligeramente diferente conocida como **Miracast Autonomous Group Owner (AGO)**. Un paso común de solución de problemas cuando se produce un error en la proyección inalámbrica a Surface Hub es probar a proyectar a otro monitor o adaptador inalámbrico. Sin embargo, en la mayoría de los casos, estos dispositivos no usan Miracast AGO y no gestiona la proyección inalámbrica del mismo modo que lo hace Surface Hub.

En el Miracast tradicional, el dispositivo de proyección conectará el punto de acceso configurado por el monitor habilitado para Miracast y luego el monitor enviará el tráfico al dispositivo de proyección mediante el canal de red del este último. Miracast AGO es un proceso de conexión de dos pasos:

- El primer paso es una conexión inicial a 2,4GHz.
- Después de ese protocolo de enlace inicial, el dispositivo de proyección envía el tráfico al monitor con la configuración de canal inalámbrico de este. Si Surface Hub está conectado a una red Wi-Fi, el punto de acceso, usará el mismo canal que la red conectada, de lo contrario usará el canal de Miracast que se indica en la configuración.

Por lo general, hay dos tipos de problemas con Miracast a Surface Hub: conexión y rendimiento. En cualquier caso, es una buena idea obtener una imagen general de la actividad de la red inalámbrica en la ubicación del Surface Hub. Si ejecutas una herramienta de análisis de red, verás las redes disponibles y el uso de canal del entorno.

Problemas de conexión

Asegúrate de que Wi-Fi y Miracast están habilitados en la configuración de Surface Hub.

Si ejecutaste un análisis de red, deberías ver Surface Hub Miracast en la lista de puntos de acceso. Si la red Miracast de Surface Hub se muestra en el análisis, pero no puede verla como un dispositivo disponible, puede intentar ajustar el canal Miracast usado por Surface Hub.

Cuando Surface Hub está conectado a una red Wi-Fi, usará la misma configuración de canal que el punto de acceso Wi-Fi para su punto de acceso de Miracast. Para solucionar problemas, desconecta Surface Hub desde las redes Wi-Fi (pero mantén Wi-Fi habilitado), para que puedas controlar el canal que se usa para Miracast. Puedes seleccionar manualmente el canal de Miracast en Configuración. Tendrás que reiniciar el Surface Hub después de cada cambio. Por lo general, es recomendable usar los canales que no muestran un uso intensivo tras el análisis de la red.

También es posible que el problema de conexión sea el resultado de un problema en el dispositivo de conexión. Si el dispositivo de proyección ejecuta Windows, debería ser Windows 8.1 o una versión posterior para asegurar compatibilidad completa con Miracast. Nuevamente, para la solución de problemas, desconecta el dispositivo de proyección de las redes Wi-Fi. De este modo, se eliminará cualquier cambio de canal entre el canal de punto de acceso y el canal de Miracast establecido en Surface Hub. Asimismo, es posible que algunas opciones de configuración de directiva de grupo y del firewall estén asociadas a una red Wi-Fi.

Comprobar controladores

También es recomendable asegurarte de que los controladores y las actualizaciones más recientes estén instalados en el dispositivo de proyección. En el Administrador de dispositivos, abre el adaptador Wi-Fi y

adaptador de vídeo, y comprueba si hay una versión de controlador actualizada. Es recomendable instalar la revisión 3120232 para Surface Pro 3 y Surface Pro 4 si estos dispositivos usan un controlador Wi-Fi más antiguo.

Comprobar la compatibilidad de Miracast

A continuación, asegúrate de que Miracast se admite en el dispositivo.

1. Presiona la tecla Windows + R y escribe `dxdiag`.
2. Haga clic en "guardar toda la información".
3. Abre el archivo dxdiag.txt guardado y busca **Miracast**. Debe aparecer **Available, with HDCP**.

Comprobar el firewall

El firewall de Windows puede bloquear el tráfico de Miracast. La prueba más sencilla consiste en deshabilitar el firewall y probar la proyección. Si Miracast funciona con el firewall deshabilitado, agrega una excepción.

```
C:\Windows\System32\WUDFHost.exe
Allow In/Out connections for TCP and UDP, Ports: All.
```

Comprobar la configuración de directiva de grupo

En los dispositivos unidos a un dominio, la directiva de grupo también puede bloquear Miracast.

1. Usa la tecla Windows + R y escribe `rsop.msc` para ejecutar el complemento **Conjunto resultante de directivas**. De este modo, se mostrarán las directivas actuales que se aplican al equipo.
2. Consulta la información de **Configuración del equipo** > **Configuración de Windows** > **Configuración de seguridad** > **Directivas de red inalámbrica (IEEE 802.11)**. Debería haber una opción de configuración para las directivas de conexiones inalámbricas.
3. Haz doble clic en la configuración de las directivas conexiones inalámbricas. Aparecerá un cuadro de diálogo.
4. Abre la pestaña **Permisos de red** y selecciona **Permitir a todos crear perfiles de todos los usuarios**.

Comprobar los registros de eventos

El último lugar donde comprobar es en los registros de eventos. Los eventos de Miracast se registrarán en **Wlanautoconfig**. Esto sucede en Surface Hub y en el dispositivo de proyección. Si exporta los registros de Surface Hub, puede ver los Wlanautoconfig de Surface Hub en la carpeta **WindowsEventLog** . Los errores en el registro de eventos pueden proporcionar algunos detalles adicionales sobre dónde se produce el error de conexión.

Problemas de rendimiento

Cuando se haya conectado una proyección inalámbrica, es posible se produzcan problemas de rendimiento que provocan latencia. Esto suele ser el resultado de una saturación general del canal o de una situación que provoca cambios de canal.

En el caso de saturación del canal, consulta el análisis de red y prueba a usar canales con menos tráfico.

Los cambios de canal se producen cuando el adaptador Wi-Fi necesita enviar tráfico a varios canales. Algunos canales admiten la selección de frecuencia dinámica (DFS). DFS se usa en los canales 49 a 148. Algunos controladores Wi-Fi tendrán un rendimiento deficiente cuando se conectan a un canal DFS. Si experimentas un rendimiento deficiente de Miracast mientras estés conectado a un canal DFS, prueba a realizar la proyección en un canal que no sea DFS. Tanto Surface Hub y como el dispositivo proyección deben usar canales no DFS.

Si Surface Hub y el dispositivo de proyección están conectados a Wi-Fi, pero con distintos puntos de acceso con diferentes canales, Surface Hub y el dispositivo de proyección estará obligado a cambiar de canal mientras está conectado Miracast. Esto resultará en una proyección inalámbrica deficiente y un rendimiento de red deficiente a través de Wi-Fi. Los cambios de canal afectarán al rendimiento de todo el tráfico inalámbrico, no solo la

proyección inalámbrica.

Los cambios de canal también se producirán si el dispositivo de proyección está conectado a una red Wi-Fi con un canal diferente que el canal que Surface Hub usa para Miracast. Por lo tanto, un procedimiento recomendado es establecer el canal Miracast del Surface Hub en el mismo canal que el punto de acceso que se usa con más frecuencia.

Si hay varios puntos de acceso o redes Wi-Fi en el entorno, es inevitable que se produzcan algunos cambios de canal. Para resolver esto, es recomendable que todos los controladores Wi-Fi estén actualizados.

Ponerse en contacto con soporte técnico

Si tiene alguna pregunta o necesita ayuda, puede crear una solicitud de soporte técnico.

Resumen

12/01/2022 • 2 minutes to read

En cumplimiento de las normativas gubernamentales regionales, todos los dispositivos inalámbricos de 5 GHz en Europa, Japón e Israel no admiten la banda U-NII-3. En Surface Hub, los canales asociados con U-NII-3 son de 149 a 165. Esto incluye la conexión Miracast en estos canales. Por lo tanto, Surface Hub que se usan en Europa, Japón e Israel no pueden usar los canales 149 a 165 para conexiones Miracast.

Más información

Para obtener más información, consulte el tema U-NII en Wikipedia.

> **NOTE**
> Microsoft proporciona información de contacto de terceros para ayudarle a encontrar información adicional sobre este tema. Esta información puede cambiar sin previo aviso. Microsoft no garantiza la precisión de la información de terceros.

Qué hacer si la aplicación Connect de Surface Hub se cierra inesperadamente

12/01/2022 • 2 minutes to read

En ocasiones, una sesión de conexión por cable que se inicia desde la pantalla de bienvenida mediante la conexión de una entrada de DisplayPort saldrá a la pantalla de bienvenida después de usar el teclado lateral o el botón de origen para desplazarse por todas las entradas de origen.

Esto es un problema de la aplicación conectar y su estado predeterminado de pantalla completa. Al cambiar el tamaño de la aplicación o al seleccionar una miniatura de entrada de DisplayPort en la aplicación conectar, puede evitar que los ciclos de entrada afecten a la aplicación.

La manera de resolver este problema es iniciar primero la aplicación Connect desde la pantalla de inicio de sesión y, a continuación, conectar una entrada de DisplayPort. Si la entrada ya está conectada, seleccione manualmente la miniatura.

Surface Hub puede instalar actualizaciones y reiniciar fuera del horario de mantenimiento

12/01/2022 • 2 minutes to read

En determinadas circunstancias, Surface Hub las actualizaciones durante el horario laboral en lugar de durante la ventana de mantenimiento normal. A continuación, el dispositivo se reinicia si es necesario. No puedes usar el dispositivo hasta que se complete el proceso.

> **NOTE**
> Este no es un comportamiento esperado por falta de una ventana de mantenimiento. Solo se produce si el dispositivo está fuera de fecha durante mucho tiempo.

Causa

Para garantizar que Surface Hub esté disponible para su uso durante el horario comercial, el concentrador está configurado para realizar funciones administrativas durante una ventana de mantenimiento que se define en Configuración (vea "Referencias", a continuación). Durante este período de mantenimiento, el concentrador instala automáticamente las actualizaciones disponibles a través de Windows Update o Windows Update for Business (WUfB). Una vez completadas las actualizaciones, el concentrador puede reiniciarse.

Las actualizaciones solo se pueden instalar durante la ventana de mantenimiento si el Surface Hub está activado pero no está en uso o reservado. Por ejemplo, si el Surface Hub está programado para una reunión que dura 24 horas, las actualizaciones programadas para instalarse se aplazarán hasta que el concentrador esté disponible durante la siguiente ventana de mantenimiento. Si el concentrador sigue ocupado y pierde varias ventanas de mantenimiento, el concentrador finalmente empezará a instalar y descargar actualizaciones. Esto puede ocurrir durante o fuera de la ventana de mantenimiento. Una vez iniciada la descarga y la instalación, el dispositivo puede reiniciarse.

Para evitar este problema

Es importante que reserve el tiempo de mantenimiento para Surface Hub realizar funciones administrativas. Reservar el Surface Hub durante intervalos de 24 horas o usar el dispositivo durante la ventana de mantenimiento retrasa la instalación de actualizaciones. Se recomienda no usar ni reservar el concentrador durante el período de mantenimiento programado. Se debe reservar una ventana de dos horas para la actualización.

Una opción que puede usar para controlar la disponibilidad de actualizaciones es Windows Update for Business.

Obtén más información

- Ventana de mantenimiento