Díganos qué opina sobre la experiencia de descarga del PDF.

Novedades de Microsoft 365 Lighthouse

Artículo • 09/02/2025

Estamos agregando continuamente nuevas características a Microsoft 365 Lighthouse, solucionando problemas que aprendemos y realizando cambios en función de sus comentarios. Revise este artículo para descubrir en qué hemos estado trabajando.

> **Nota**
>
> Las características se implantan a diferentes velocidades para nuestros clientes. Si aún no ve una característica, debería verla pronto.
>
> Para ver qué nuevas características están disponibles actualmente en el inquilino del partner, vaya a la página **Inicio** de Microsoft 365 Lighthouse y, a continuación, seleccione el vínculo **Novedades** de la esquina superior derecha de la página o seleccione **Novedades** de la tarjeta **Novedades y recursos de aprendizaje**.

Enero de 2025

Creación de un informe de cliente de "Resumen ejecutivo"

Ahora puede generar un informe para cada inquilino de cliente en Microsoft 365 Lighthouse que resalta áreas clave en torno a la posición de seguridad y el estado empresarial. El informe también resume las actividades clave que la organización asociada realizó en Lighthouse para mantener a los clientes seguros, seguros y productivos.

Hemos oído hablar de usted sobre la necesidad de compartir un informe con sus clientes durante las revisiones empresariales mensuales o trimestrales y este resumen ejecutivo es el primer paso para crear las vistas de un extremo a otro necesarias para garantizar que las revisiones con los clientes sean lo más productivas posible.

Para generar un informe de cliente, en el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos** y, a continuación, seleccione cualquier inquilino de la lista para abrir la página de detalles del inquilino. Desde allí, seleccione la pestaña **Información general** , seleccione **Resumen** en el panel izquierdo y, a continuación, seleccione **Crear informe**.

Vaya a la página Inquilinos ahora (una vez allí, seleccione un inquilino)

Para obtener más información, consulte Creación de un informe de cliente en Microsoft 365 Lighthouse.

Diciembre de 2024

Visualización de todas las licencias comerciales para un inquilino de cliente

Ahora puede acceder a información sobre todas las licencias adquiridas por un cliente en varias suscripciones comerciales de Microsoft. Tenga en cuenta que esta información del producto está restringida a las suscripciones adquiridas a través de la nueva experiencia comercial en el programa Proveedor de soluciones en la nube (CSP) y no incluye suscripciones de Microsoft Azure.

Para cada SKU comprada por el cliente, puede ver las licencias de pago y las licencias sin asignar. Puede usar esta vista completa del perfil de licencia del inquilino del cliente para ayudar a los clientes a maximizar el valor de sus suscripciones de Microsoft.

Para acceder a la información de licencia de un inquilino de cliente, en el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos** y, a continuación, seleccione cualquier inquilino de la lista para abrir la página de detalles del inquilino. Desde aquí, seleccione la pestaña **Detalles del producto y uso** y, a continuación, seleccione **Licencias** en el panel izquierdo.

Vaya a la página Inquilinos ahora (una vez allí, seleccione un inquilino)

Se ha actualizado la configuración de la tarea de implementación "Requerir MFA para administradores".

A medida que los roles y permisos de Microsoft 365 Lighthouse han evolucionado para reducir el riesgo de seguridad para usted y sus clientes, hemos actualizado la configuración subyacente de la tarea de implementación "Requerir MFA para administradores" en la línea base predeterminada para tener en cuenta las siguientes asignaciones de roles Microsoft Entra:

- Administrador de la aplicación
- Administrador de aplicaciones en la nube
- Administrador de contraseñas
- Administrador de autenticación con privilegios

- Administrador de roles con privilegios

Esta actualización puede cambiar el estado de cumplimiento de la subtarea "Crear directiva de acceso condicional para requerir MFA para administradores" a **No compatible** para algunos inquilinos de clientes. Para garantizar que los inquilinos permanezcan seguros, se recomienda volver a implementar la subtarea para volver a cumplirla.

Para volver a implementar la subtarea, vaya a la página **Inquilinos** , seleccione el inquilino y, a continuación, seleccione la pestaña **Plan de implementación** . Busque y expanda la tarea "Requerir MFA para administradores", seleccione la subtarea "Crear directiva de acceso condicional para requerir MFA para administradores" y, a continuación, seleccione **Implementar**.

Si previamente clonó la tarea de implementación "Requerir MFA para administradores" como parte de las líneas base personalizadas, deberá volver a clonar la tarea actualizada para cada una de esas líneas base personalizadas.

Con esta actualización, la pestaña **Historial de detección** muestra datos basados en la subtarea actualizada. El historial de detección basado en la subtarea actualizada previamente ya no está disponible.

Para obtener más información, consulte Requerir MFA para administradores: Microsoft Entra ID.

Oportunidades específicas del inquilino para la interacción

Microsoft 365 Lighthouse ahora incluye información y recomendaciones para los inquilinos del cliente en la página de detalles del inquilino. Puede ver una lista de oportunidades disponibles para el inquilino seleccionado, exportar la lista de oportunidades a un archivo .CSV o ver oportunidades para todos los inquilinos de clientes a través de un vínculo conveniente.

Ver estas oportunidades, en función del valor potencial, el riesgo y la preparación, en contexto con otros datos clave, como el uso y las suscripciones de aplicaciones y servicios, facilita la revisión y priorización de información procesable, lo que puede ayudarle a interactuar con sus clientes.

Para acceder a las oportunidades de un inquilino de cliente, en el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos** y, a continuación, seleccione un inquilino de la lista. En la página de detalles del inquilino, seleccione la pestaña **Detalles del producto y uso** y, a continuación, seleccione **Oportunidades** en el panel izquierdo.

Vaya a la página Inquilinos ahora (una vez allí, seleccione un inquilino)

Noviembre de 2024

Nuevos roles de RBAC de Lighthouse para administrar permisos de inquilino de asociados

Microsoft 365 Lighthouse ahora incluye los siguientes roles de control de acceso basado en rol (RBAC) que puede usar para administrar los permisos de inquilino de asociados en Lighthouse. Para asignar estos roles, debe ser administrador de Lighthouse o administrador de roles con privilegios en Microsoft Entra ID en el inquilino del asociado.

- Administrador de cuentas de Lighthouse
- Administrador de Lighthouse
- Autor de Lighthouse
- Operador Lighthouse (asignado automáticamente a usuarios con permisos GDAP para un inquilino de cliente)
- Lector de Lighthouse

Cada rol tiene un conjunto de permisos que determina a qué usuarios de datos pueden acceder y cambiar dentro del inquilino del asociado. Por ejemplo, puede asignar el rol Administrador de cuentas de Lighthouse a los usuarios que requieren acceso a Sales Advisor.

Para asignar roles de RBAC, en el panel de navegación izquierdo de Lighthouse, seleccione **Permisos permisos**>**de Lighthouse**.

Ir ahora a la página permisos de Lighthouse.

Para obtener más información, consulte Información general sobre los permisos en Microsoft 365 Lighthouse.

Nueva tarjeta de página principal para empezar a trabajar rápidamente con Lighthouse

Nos complace presentar un nuevo **Let's start with the basics card on the Home page (Empezar con la tarjeta de conceptos básicos** en la página **principal**). Cuando un usuario inicia sesión en Microsoft 365 Lighthouse, la nueva tarjeta identifica las tareas clave y los recursos de aprendizaje (con el ámbito del rol o roles de RBAC de Lighthouse asignados por el usuario) para ayudarle a configurar sus cuentas y conocer los conceptos básicos de Lighthouse.

La nueva tarjeta contiene una lista de tareas pertinentes y guías interactivas en forma de lista de comprobación. Al seleccionar un elemento de la lista, se inicia simultáneamente la tarea o el recurso y se marca el elemento como iniciado, lo que facilita a los usuarios realizar un seguimiento de su progreso.

La tarjeta Comencemos con los conceptos básicos es una excelente manera de que los nuevos usuarios se ponga al día rápidamente y se sientan cómodos con Lighthouse, de modo que puedan trabajar de forma más eficaz con los clientes para mantenerlos seguros, seguros y productivos. La tarjeta también beneficia a los usuarios existentes de Lighthouse al servir como un actualizador útil.

Para empezar, vaya a la página **Principal** de Lighthouse, busque la tarjeta **Comencemos con los conceptos básicos** y, a continuación, seleccione un elemento de la lista de la tarjeta.

Vaya a la página principal ahora

Octubre de 2024

Acceder fácilmente a los detalles del inquilino desde cualquier página de Lighthouse

Le hemos facilitado el acceso a los detalles del inquilino del cliente desde cualquier página de Lighthouse. Anteriormente, tenía que ir a la página **Inquilinos** y, a continuación, seleccionar un inquilino de la lista para ver los detalles de ese inquilino. Ahora, al seleccionar un inquilino en el filtro **Inquilinos** en cualquier página, aparece un vínculo junto al filtro que le lleva directamente a la página de detalles del inquilino seleccionado. Esta funcionalidad le ayuda a administrar de forma más eficaz los inquilinos de los clientes, ya que le proporciona acceso con un solo clic a la información importante del inquilino, independientemente de dónde se encuentren en Lighthouse.

Septiembre de 2024

Página de acceso delegado

Hemos simplificado la administración de privilegios administrativos delegados granulares (GDAP) en Microsoft 365 Lighthouse mediante la eliminación de la herramienta de instalación de GDAP y su reemplazo por la página **Acceso delegado**. Esta nueva página le permite hacer lo siguiente:

- Cree y asigne plantillas de Lighthouse GDAP a inquilinos de clientes de forma masiva o singular.
- Administrar grupos de seguridad con permisos GDAP.
- Vea el estado de las relaciones de GDAP con los clientes.
- Identifique la fecha de expiración más cercana de cada relación GDAP.

Para crear grupos de seguridad, debe ser administrador de grupos en el inquilino del asociado. Para cambiar la pertenencia de usuario en grupos, debe ser administrador de usuarios en el inquilino del asociado. Para crear relaciones GDAP, debe ser un agente de Administración en el Centro de partners.

Para acceder a la página **Acceso delegado** , en el panel de navegación izquierdo de Lighthouse, seleccione **Permisos**>**de acceso delegado**.

Vaya a la página Acceso delegado ahora

Para obtener más información sobre cómo configurar GDAP, consulte Configuración de GDAP en Microsoft 365 Lighthouse.

Para obtener más información sobre el acceso delegado, consulte Información general de la página Acceso delegado en Microsoft 365 Lighthouse.

Uso de la información de Copilot en Lighthouse para impulsar el éxito de Copilot

La nueva página **de conclusiones de Copilot** le permite administrar y supervisar fácilmente el éxito de Copilot en los inquilinos de sus clientes, todo en un solo lugar. Además de recomendar a los clientes que es probable que encuentren valor en Copilot, la página muestra el uso y la asignación de licencias de Copilot y proporciona vínculos a recursos clave para que pueda convertirse en un experto de Copilot, incluidos Galería de consultas de Copilot, rutas de aprendizaje y vídeos de entrenamiento. En la página también se muestra el progreso de la implementación de las tareas que se recomiendan específicamente para habilitar Copilot.

Además, la información de Copilot le ayuda a identificar a los clientes que pueden necesitar orientación o entrenamiento de configuración de Copilot. Use la información para asegurarse de que todos los usuarios de Copilot están habilitados y configurados para que se realicen correctamente.

Para acceder a esta nueva página, en el panel de navegación izquierdo de Lighthouse, seleccione **Copilot Insights**.

Vaya ahora a la página de conclusiones de Copilot.

Nueva tarea de implementación de línea base predeterminada para habilitar la transcripción de Microsoft Teams

Hemos agregado una nueva tarea de implementación a la línea base predeterminada que le permite habilitar la transcripción automática en Microsoft Teams en el inquilino del cliente.

La transcripción permite a los usuarios reproducir grabaciones de reuniones con subtítulos y revisar elementos de discusión importantes en la transcripción. La transcripción y los subtítulos ayudan a crear contenido inclusivo para los espectadores.

Clone esta nueva tarea de implementación para agregarla a la línea base personalizada y, a continuación, vaya al plan de implementación del inquilino del cliente para implementar la configuración.

Para obtener más información sobre la transcripción y los subtítulos, consulte Administración de transcripciones y subtítulos para reuniones de Teams.

Agosto de 2024

Acceso a la información de almacenamiento del buzón desde la página de detalles del inquilino

Nuestra página de detalles de inquilino mejorada ahora le permite realizar un seguimiento del uso del almacenamiento de buzones de correo para los usuarios y los buzones compartidos en los inquilinos del cliente. Esta característica proporciona información sobre el consumo de almacenamiento, lo que ayuda a la optimización y planeación de recursos de licencia.

Para acceder a la información de almacenamiento del buzón de correo, en el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos** y, a continuación, seleccione cualquier inquilino de la lista para abrir la página de detalles del inquilino. Desde allí, seleccione la pestaña **Información general** o **la pestaña Usuarios** y, a continuación, seleccione **Uso del almacenamiento de buzones**.

Vaya a la página Inquilinos ahora (una vez allí, seleccione un inquilino)

Mejoras de alertas

Las reglas de alertas de Microsoft Defender para punto de conexión alertas ahora incluyen la opción de filtrar por estado de alerta. Puede actualizar las reglas de alerta existentes para excluir las alertas de punto de conexión **resueltas** .

Para reducir la probabilidad de reactivación, una alerta de Microsoft 365 Lighthouse en estado **Descartado** ya no se moverá al estado **Resuelto**.

Vaya a la página Alertas ahora

Para obtener más información, consulte Información general de la página Alertas de Microsoft 365 Lighthouse.

Junio de 2024

Acceder a la información clave desde la página mejorada de detalles del inquilino

Estamos encantados de anunciar una importante actualización de la página de detalles del inquilino que le permite acceder a información clave relacionada con los inquilinos de sus clientes desde un único lugar. Ya no es necesario ver varias páginas para obtener información básica. Nuestra sección de **Información de clientes** renovada proporciona un lugar centralizado para realizar el seguimiento de los datos clave de los clientes y las notas para ayudarle a mantenerse proactivo y optimizar los recursos.

¿Se pregunta cuánto almacenamiento consumen los usuarios del inquilino del cliente? Ahora puede supervisar el uso del almacenamiento del buzón desde la página de detalles del inquilino. ¿Desea supervisar fácilmente las suscripciones de Microsoft que ha vendido a los clientes? Vea los detalles de la suscripción, las fechas de renovación y los servicios asociados, todo en un solo lugar.

Además, en los próximos meses se implementarán aún más mejoras:

- Navegación rápida: vaya directamente a la página de detalles de cualquier inquilino desde cualquier página de Lighthouse.
- Informe orientado al cliente: prepárese para una característica muy esperada: un informe completo que puede compartir directamente con sus clientes.
- Y mucho más... permanezca atento.

Para comprobar las mejoras recientes, en el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos** y, a continuación, seleccione cualquier inquilino de la lista para abrir la página de detalles del inquilino.

Vaya a la página Inquilinos ahora (una vez allí, seleccione un inquilino para ver la página de detalles del inquilino mejorado)

Mayo de 2024

Página de detalles del inquilino mejorada

Hemos mejorado la página de detalles del inquilino para proporcionar una vista más completa de los detalles del inquilino del cliente. Publicaremos estas mejoras en fases durante los próximos meses. La página de detalles de inquilino mejorada incluye una pestaña **Información general** rediseñada que tiene una sección **Resumen** que muestra información de alto nivel sobre el progreso de la implementación de línea base y las alertas, y una sección de **Información de cliente** expandida donde puede registrar notas sobre el cliente para facilitar la colaboración con sus compañeros. También hemos agregado una pestaña **Acciones** donde puede ver las tareas resumidas para el inquilino que requieren su atención. Esta nueva pestaña incluye vínculos a las páginas relevantes para realizar las tareas, lo que ofrece una manera sencilla de ver los detalles y tomar medidas.

Para comprobar estas mejoras, en el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos** y, a continuación, seleccione cualquier inquilino de la lista para abrir la página de detalles del inquilino y ver la pestaña **Información general**. Desde allí también puede acceder a la nueva pestaña **Acciones**.

Vaya a la página Inquilinos ahora (una vez allí, seleccione un inquilino)

Abril de 2024

Actualización de requisitos de rol del administrador de cuentas RBAC de Lighthouse

Ya no es necesario tener una licencia de Microsoft Entra ID P1 para administrar el rol de administrador de cuentas RBAC de Lighthouse. Este cambio significa que los grupos de seguridad asignados al rol de administrador de cuentas RBAC de Lighthouse ya no necesitan ser un grupo al que se puedan asignar roles. Ahora puede asignar cualquier grupo de seguridad, incluidos los grupos de seguridad existentes, al rol de administrador de cuentas RBAC de Lighthouse.

Vaya ahora a la página permisos de Lighthouse.

Para obtener más información, consulte Información general sobre los permisos en Microsoft 365 Lighthouse.

Visualización y configuración de nuevos usuarios

Hemos agregado una página **Nuevos usuarios** que muestra todos los nuevos usuarios en los inquilinos administrados en Microsoft 365 Lighthouse. Puede usar esta página para realizar un seguimiento y asegurarse de que todos los usuarios incorporados recientemente en los inquilinos se han configurado correctamente con licencias, grupos y mucho más.

Para acceder a esta nueva página, vaya a**Administración de**> cuentas **de usuarios**>**Nuevos usuarios**. La página **Nuevos usuarios** también le permite agregar rápidamente un nuevo usuario a cualquiera de los inquilinos.

Vaya a la página Nuevos usuarios ahora.

Uso de aplicaciones y servicios en la página Inquilinos

Hemos agregado una nueva columna a la página **Inquilinos** de Microsoft 365 Lighthouse que muestra el uso de aplicaciones y servicios de cada cliente. Esto le ayuda a identificar a los clientes que no están aprovechando todo el potencial de Microsoft 365 y que podrían necesitar su orientación o asistencia. La columna muestra el estado de uso de cuatro cargas de trabajo principales: aplicaciones principales de Microsoft (Word, Excel, PowerPoint y OneNote), Teams, almacenamiento (SharePoint o OneDrive) y correo electrónico (Exchange). Un cliente que tiene una adopción muy baja o nula de cualquiera de estas cargas de trabajo se marca como no incorrecto. Puede utilizar esta información para priorizar sus acciones y llegar a aquellos clientes que necesiten más asistencia o ayuda para configurar su suscripción a Microsoft 365.

Para acceder a esta funcionalidad, en el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos** y, a continuación, consulte la columna **Aplicaciones & uso de servicios** en la página **Inquilinos**.

Ir a la página Inquilinos ahora

Para más información, consulte Información general sobre el modelo de páginas de SharePoint.

Administrar estado de la aplicación Microsoft 365 desde Lighthouse

El nuevo informe de administración de aplicaciones le permite supervisar y administrar fácilmente el estado de la aplicación Microsoft 365 en los inquilinos del cliente. Por ejemplo, puede comprobar si los dispositivos del cliente tienen habilitada la actualización en la nube, lo que garantiza que las aplicaciones estén siempre actualizadas. El informe también identifica qué canales de aplicaciones de Microsoft 365 están implementados en los inquilinos de clientes que tienen habilitado el servicio de inventario en el Centro de administración de Aplicaciones de Microsoft 365 y a través de qué canales de aplicación los clientes reciben las actualizaciones.

Además, el informe de administración de aplicaciones permite determinar fácilmente si los clientes están ejecutando versiones de Office no conformes o si todavía no tienen la última versión. Esto le ayuda a identificar de forma proactiva los posibles problemas de usuario final que podrían surgir al usar versiones de Office que no están actualizadas. Esta información está disponible para todos los clientes con dispositivos Win32; no hay ningún requisito de Intune en el inquilino del cliente.

Para acceder a este nuevo informe, vaya a**Aplicaciones**>**Administración de aplicaciones**.

Vaya a la página Administración de aplicaciones ahora

Marzo de 2024

Widget de comentarios y soporte técnico

Le hemos facilitado la tarea de hacernos llegar sus comentarios. Consulte los nuevos comentarios y el widget de soporte técnico en la esquina inferior derecha del portal de Lighthouse. Haga una sugerencia, notifique un problema o haga un cumplido simplemente seleccionando el widget. Comparta sus comentarios hoy a través de nuestra herramienta de comentarios mejorados y háganos saber cómo Lighthouse está funcionando para usted.

Febrero de 2024

Administración de scripts de PowerShell

Ahora puede crear scripts de PowerShell y comprobar los resultados de los dispositivos administrados por Intune en Microsoft 365 Lighthouse en lugar de tener que ir a la página Scripts del dispositivo en el Centro de administración de Microsoft Intune para cada cliente. Para acceder a esta funcionalidad, seleccione **Inquilinos** en el panel de

navegación izquierdo de Lighthouse, seleccione un inquilino de la lista y, a continuación, seleccione la pestaña **Scripts**.

Para crear un script, seleccione **Crear script**. Para ver una lista de dispositivos de destino y el último tiempo de ejecución de un script existente, seleccione un script de la lista. Puede ejecutar scripts en todos los dispositivos administrados por Intune en un inquilino de cliente o puede seleccionar dispositivos mediante grupos de Microsoft Entra.

Enero de 2024

Seguimiento de las próximas renovaciones de suscripción

Para ayudarle a priorizar e impulsar las discusiones de renovación de suscripciones con los clientes de forma más eficaz, hemos agregado una página a Microsoft 365 Lighthouse que le permite realizar un seguimiento de las suscripciones de clientes que expiran en los próximos 90 días.

Para acceder a esta nueva página, en el panel de navegación izquierdo de Lighthouse, seleccione **Sales Advisor (Project Orland)** > **Próximas renovaciones**.

Si no está familiarizado con Sales Advisor, debe ser administrador de cuentas de Lighthouse en el inquilino del partner para acceder a la página **Próximas renovaciones**. Para obtener más información, consulte Introducción a los permisos en Microsoft 365 Lighthouse. Si ya tiene acceso a Sales Advisor, no necesita el rol Administrador de cuentas de Lighthouse en este momento.

En la página **Próximas renovaciones** se enumeran todas las suscripciones de clientes, ordenadas por fecha de expiración de la suscripción. Puede ordenar y filtrar la lista por fecha de expiración, frecuencia de facturación, estado de facturación periódica, número de licencias y mucho más. Para facilitar la visualización de todas las suscripciones que expiran para cada inquilino, cambie a la vista **Lista de grupos por inquilino**.

Ir a la página próximas renovaciones ahora

Para obtener más información, consulte "Optimizar las conversaciones de renovación con información de renovación simplificada" en la Entrada de blog: Desbloquear la oportunidad de Copilot y hacer crecer su negocio de CSP con Microsoft 365 Lighthouse.

Oportunidades de Microsoft Copilot en Sales Advisor

Hemos agregado Microsoft Copilot oportunidades a Sales Advisor para ayudarle a identificar a los clientes que son aptos para comprar Microsoft 365 Copilot. Microsoft Copilot es un complemento de IA que funciona en todas partes y se adapta de forma inteligente a sus necesidades.

Para acceder a las oportunidades de Copilot, en el panel de navegación izquierdo de Microsoft 365 Lighthouse, seleccione **Sales Advisor (Project Orland)** > **Oportunidades** y, a continuación, seleccione la pestaña **Crecimiento del cliente**.

Seleccione una oportunidad de Copilot para ver la información del cliente, las acciones sugeridas y los recursos para interactuar con el cliente.

Ir a la página Oportunidades ahora

Para obtener más información, consulte la Entrada de blog: Desbloquear la oportunidad de Copilot y hacer crecer su negocio de CSP con Microsoft 365 Lighthouse .

Asignar automáticamente la configuración de la plantilla de GDAP después de la aprobación del cliente de las relaciones de GDAP

Ahora puede configurar privilegios administrativos delegados pormenorizadas (GDAP) para cualquier inquilino del cliente,independientemente de la relación delegada que ya se haya configurado, sin necesidad de pasos adicionales después de activar una relación GDAP. Asigne una plantilla GDAP a cualquier inquilino de cliente en Microsoft 365 Lighthouse y, una vez que el cliente apruebe la relación, los grupos de seguridad y los roles de soporte técnico se aplicarán automáticamente. No es necesario volver a ejecutar el programa de instalación de GDAP ni realizar pasos adicionales después de activar una relación para aplicar toda la configuración de la plantilla de GDAP.

Para asignar una plantilla de GDAP, vaya a la página **Inicio** de Lighthouse y seleccione **Configurar GDAP** en la tarjeta **Configuración de GDAP**.

Ir a Configurar GDAP ahora

Para obtener más información, consulte Configurar GDAP para los clientes en Microsoft 365 Lighthouse.

Administrar el acceso de Sales Advisor con el nuevo rol Administrador de cuentas de Lighthouse

Ahora puede administrar el acceso de Sales Advisor directamente desde la página de permisos de Lighthouse en Microsoft 365 Lighthouse. Asigne el rol Administrador de cuentas de Lighthouse a los usuarios del inquilino del partner que necesiten acceso completo a las páginas de Sales Advisor, a los datos de todo el inquilino del partner y a las funcionalidades como la capacidad de exportar datos.

Para asignar el rol Administrador de cuentas de Lighthouse, vaya a **Permisos**>**Permisos de Lighthouse**.

Esté atento al anuncio de nuevos roles de administración de Lighthouse que puede usar para administrar mejor los permisos de inquilinos del partner en Lighthouse.

Ir ahora a la página permisos de Lighthouse.

Para obtener más información, consulte Información general sobre los permisos en Microsoft 365 Lighthouse.

Octubre de 2023

Información de disponibilidad de datos

Con la expansión de los inquilinos que son aptos para la administración en Microsoft 365 Lighthouse, hemos agregado información de disponibilidad de datos a nuestras páginas de administración para que sepa si ve datos completos, datos parciales o ningún dato. Lighthouse también le ayuda a comprender por qué pueden faltar o estar incompletos los datos para algunos de los inquilinos del cliente y qué pasos puede seguir para obtener visibilidad completa.

Estas conclusiones evitan la suposición de que los inquilinos que no se notifican son correctos y seguros cuando esos datos realmente no están disponibles para Lighthouse.

La información de disponibilidad de datos se ha agregado a las páginas siguientes:

- Autenticación multifactor
- Usuarios de riesgo
- Restablecimiento de contraseña
- Protección de datos
- Cumplimiento de dispositivos
- Estado del dispositivo
- Seguridad de dispositivos
- Administración de amenazas
- Administración de amenazas y vulnerabilidades

Para ver la información, vaya a cualquiera de estas páginas en Lighthouse.

Septiembre de 2023

Registros de eventos de Windows

La página **Registros de eventos de Windows** de Microsoft 365 Lighthouse usa inteligencia artificial (IA) para generar sugerencias para mitigar los problemas que se encuentran en los registros de eventos de Windows. La línea base "Recopilar registros de eventos de Windows" permite la recopilación de registros de eventos de dispositivos administrados. Una vez ingeridos los registros, puede verlos seleccionando **Dispositivos**>**Registros de eventos de Windows** en el panel de navegación izquierdo de Lighthouse. Para ver detalles adicionales, seleccione cualquier entrada de registro.

Ir ahora a la página Registros de eventos de Windows.

Acciones rápidas en la página principal

Ahora puede realizar acciones comunes, como agregar un nuevo usuario, etiquetar los inquilinos, acceder a otros centros de administración y mucho más desde la página principal de Microsoft 365 Lighthouse. La nueva barra de comandos de la parte superior de la página principal le ayuda a encontrar y realizar estas acciones siempre que las necesite.

Agosto de 2023

Puntuación de seguridad de Microsoft

La Puntuación de seguridad de Microsoft, que es una representación de la posición de seguridad de una organización, se integra ahora en Microsoft 365 Lighthouse. Lighthouse proporciona una vista agregada de la Puntuación de seguridad en todos los inquilinos administrados, así como detalles de Puntuación de seguridad para cada inquilino individual. Puede acceder a la Puntuación de seguridad a través de una nueva tarjeta en la página **Inicio** o seleccionando un inquilino en la página **Inquilinos**. Una vez que seleccione un inquilino, seleccione la pestaña **Puntuaciones** para ver los datos históricos de puntuación de seguridad del inquilino.

Para más información, consulte Puntuación de seguridad de Microsoft.

Alertas en Microsoft 365 Lighthouse

Microsoft 365 Lighthouse ahora proporciona una vista consolidada de alertas con prioridad para que pueda ver rápidamente las alertas principales sobre las que debe actuar en todos los inquilinos administrados. También puede configurar reglas de alerta basadas en los datos de Lighthouse, lo que le permite priorizar los elementos que necesitan atención inmediata.

Lighthouse también admite ahora la capacidad de configurar alertas push personalizadas para permitir la integración con los sistemas de vales y soporte técnico existentes.

Para acceder a esta funcionalidad, en el panel de navegación izquierdo de Lighthouse, seleccione **Alertas**.

Para obtener más información, consulte Información general de la página Alertas de Microsoft 365 Lighthouse.

Julio de 2023

Sales Advisor ahora forma parte de Microsoft 365 Lighthouse

Sales Advisor, anteriormente conocido como Project Orland en Insights del Centro de partners, ahora está integrado en Microsoft 365 Lighthouse.

Sales Advisor le ayuda a aprovechar el poder de la información basada en inteligencia artificial para impulsar el crecimiento empresarial y ofrecer servicios administrados escalables a sus clientes. Con Sales Advisor, puede detectar recomendaciones proactivas, accionables y personalizadas para adquirir nuevos clientes, aumentar la retención de clientes y expandir su negocio con ofertas premium.

Para ver El Asesor de ventas en Lighthouse, en el panel de navegación izquierdo, seleccione **Sales Advisor**>**Oportunidades**. Para obtener más información, consulte Información general de Sales Advisor Microsoft 365 Lighthouse.

Junio de 2023

Tarea de implementación para administrar actualizaciones de Windows

Ahora puede implementar directivas de implementación de actualizaciones de Windows para asegurarse de que los dispositivos de inquilinos del cliente tengan las revisiones de seguridad, correcciones de errores y mejoras de rendimiento más recientes. También obtendrá información sobre qué inquilinos no tienen las directivas de implementación de actualizaciones de Windows, qué inquilinos están en proceso de implementar las directivas y cuáles las han implementado correctamente.

Para obtener más información, consulte Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar.

Acceso a centros de administración desde Lighthouse

Hemos agregado vínculos del Centro de administración a Microsoft 365 Lighthouse para que pueda administrar sus clientes de forma más eficaz. Los vínculos del centro de administración le permiten ir directamente desde Lighthouse al Centro de administración correspondiente para el inquilino del cliente seleccionado.

Puede acceder a los vínculos del Centro de administración desde la página **Inquilinos** o mediante el filtro **Inquilinos** que está disponible en Lighthouse. En la página **Inquilinos**, seleccione los tres puntos (más acciones) junto al inquilino del cliente cuyos servicios desea administrar y, a continuación, seleccione **Administrar servicios** para abrir la lista de vínculos del Centro de administración. Para usar el filtro **Inquilinos**, abra el filtro, busque el inquilino del cliente cuyos servicios desea administrar y, a continuación, seleccione el símbolo > junto al nombre del inquilino para abrir la lista de vínculos del Centro de administración.

Para obtener más información, consulte Información general de la página Inquilinos en Microsoft 365 Lighthouse.

"Novedades" ahora está personalizada para el inquilino

Dado que las nuevas características se implementan gradualmente en los partners de Microsoft 365 Lighthouse, hemos cambiado nuestras notificaciones "Novedades" para informarle cuando hay nuevas características disponibles en el inquilino del partner.

Para ver qué nuevas características están disponibles en el inquilino del partner, vaya a la página **Inicio** de Lighthouse y, a continuación, seleccione el vínculo **Novedades** de la esquina superior derecha de la página o seleccione **Novedades** en la tarjeta **Novedades y recursos de aprendizaje**.

Para obtener una lista completa de las características más recientes de Lighthouse, que pueden o no estar disponibles aún en el inquilino del partner, consulte la lista de este

artículo.

Usuarios de riesgo para todos los inquilinos

La página **Usuarios de riesgo** se ha actualizado para mostrar información de usuario de riesgo para todos los inquilinos de clientes incorporados, incluso si los inquilinos del cliente no tienen Azure Active Directory Premium P1 o superior. Por ejemplo, si un inquilino solo tiene una licencia para Microsoft Defender para Empresas o Windows 365 Business, podrá ver las cuentas de usuario marcadas por comportamientos de riesgo en ese inquilino.

Para ver esta funcionalidad actualizada, en el panel de navegación izquierdo de Microsoft 365 Lighthouse, seleccione **Usuarios**>**Usuarios de riesgo**.

Ir ahora a la página Usuarios de riesgo.

Para obtener más información, consulte Visualización y administración de usuarios de riesgo en Microsoft 365 Lighthouse.

Métricas de usuario detalladas

Ahora puede ver métricas detalladas de todas las cuentas de usuario administradas si va a **Usuarios**>**Administración de cuentas**>**Métricas de usuario**. Puede ver cuántos usuarios, usuarios con licencia, usuarios invitados, administradores globales, usuarios inactivos y buzones compartidos desbloqueados tiene en los inquilinos del cliente. Estos datos pueden ayudarle a administrar las cuentas de usuario de forma más eficaz y eficiente para mantener la integridad de los inquilinos de los clientes.

En la página **Métricas de usuario**, también puede acceder rápidamente al Centro de administración de Microsoft 365, donde puede ver información completa del usuario y realizar acciones adicionales.

Para obtener más información, consulte Información general de la página Usuarios en Microsoft 365 Lighthouse.

Mayo de 2023

La configuración de GDAP ahora comprueba si hay roles necesarios

Hemos actualizado la configuración de GDAP en Microsoft 365 Lighthouse para comprobar si tiene los roles necesarios antes de empezar. Si no tiene los roles necesarios, un mensaje le avisará.

Para acceder al programa de instalación de GDAP en Lighthouse, vaya a la tarjeta **Configuración de GDAP** en la página **Inicio** y, a continuación, seleccione **Configurar GDAP**.

Para obtener más información, consulte Configurar GDAP para los clientes en Microsoft 365 Lighthouse.

Abril de 2023

Informes de desfase de configuración

Microsoft 365 Lighthouse ahora tiene la capacidad de identificar las tareas de implementación que han retrocedido (o se han desviado) de un estado *Conforme* o *Descartado* a un estado de *No conforme* o *Sin licencia*.

Las tareas de implementación pueden derivar de un estado preferido por cualquier razón que puede ser difícil de detectar. Comprender cómo la configuración de un inquilino del cliente se ha desviado del estado preferido puede ser un proceso complejo y con mucha mano de obra.

Microsoft 365 Lighthouse no solo le permite saber qué tareas de implementación se han desviado de los planes de implementación de los inquilinos, sino cuáles ajustes, dentro de cuáles configuraciones y para cuáles usuarios, se han desviado del estado preferido para que pueda restaurar el inquilino de forma eficaz y eficiente a un estado correcto, productivo y seguro.

Adición de la configuración de Sincronización de OneDrive a los planes de implementación

Ahora puede implementar directivas de OneDrive mediante una tarea de implementación dentro de la línea base predeterminada. La adición de esta configuración ayuda a proteger los datos de los inquilinos del cliente mediante la restricción de la sincronización en OneDrive para los usuarios autenticados correctamente.

Nuevas funcionalidades de administración de GDAP

Los técnicos del proveedor de servicios administrados (MSP) responsables de administrar los privilegios administrativos delegados granulares (GDAP) ahora pueden obtener detalles de un vistazo de todas las relaciones delegadas de sus clientes en Microsoft 365 Lighthouse. Esta nueva funcionalidad ayuda a garantizar que GDAP esté configurado correctamente para todos los clientes.

Para ver el estado de las relaciones delegadas de los clientes, incluido el tipo de acceso delegado, si se ha asignado una plantilla GDAP, el número de relaciones activas y pendientes, la fecha de expiración más cercana y los grupos de seguridad con acceso para administrar el inquilino del cliente, vaya a **Permisos**>**Acceso delegado**.

Marzo de 2023

Administración de amenazas y vulnerabilidades multiinquilino de Microsoft Defender para punto de conexión

La Administración de vulnerabilidades de Microsoft Defender ayuda a identificar y crear de forma proactiva una base segura para los dispositivos a través de la corrección de vulnerabilidades de software y configuraciones incorrectas en entornos de cliente. Microsoft 365 Lighthouse ahora incluye funcionalidades de administración de vulnerabilidades. Vaya a **Dispositivos**>Administración de vulnerabilidades para ver la puntuación de exposición en todos los inquilinos administrados que se han incorporado a Microsoft Defender para punto de conexión. Para ver recomendaciones de seguridad sobre cómo reducir la exposición de los inquilinos a vulnerabilidades, seleccione la pestaña **Recomendaciones**.

Información de seguridad de dispositivos de Microsoft Defender para Empresas y Microsoft Defender para punto de conexión

Microsoft 365 Lighthouse ahora muestra información resumida sobre las distintas alertas de seguridad de Microsoft Defender para Empresas y Microsoft Defender para punto de conexión en los inquilinos administrados. Para acceder a estas conclusiones, vaya a **Dispositivos**>**Dispositivos de seguridad**>Información general. Estas conclusiones pueden ayudarle a evaluar el estado general, la gravedad y la categoría de las distintas alertas de seguridad de los inquilinos antes de profundizar en la lista completa de alertas.

Mejoras en la página Inquilinos

Hemos actualizado la página Inquilinos para ayudarle a administrar más fácilmente los inquilinos de los clientes en Microsoft 365 Lighthouse. Con la nueva característica Opciones de lista, a la que tiene acceso seleccionando el icono situado junto al cuadro de búsqueda, ahora puede ver los inquilinos del cliente por nombre de dominio o identificador de inquilino. También hemos actualizado la página Inquilinos para reflejar la nueva configuración de privilegios administrativos delegados granulares (GDAP) y las funcionalidades de administración de Lighthouse.

Observará que los inquilinos de clientes que no cumplen los criterios para administrarse completamente en Microsoft 365 Lighthouse (por ejemplo, no tienen GDAP configurado o no tienen una suscripción necesaria) muestran un estado de administración de Lighthouse **Limitado**. Estos inquilinos solo son aptos para un conjunto limitado de experiencias en Microsoft 365 Lighthouse, incluida la configuración y administración de GDAP, la búsqueda de usuarios, los detalles del usuario, el etiquetado de inquilinos y el estado del servicio.

Por último, hemos agregado un nuevo panel que detalla los criterios del cliente para cada uno de los inquilinos del cliente. Para los clientes con un estado de administración **Limitado** de Lighthouse, por ejemplo, puede seleccionar el nombre del inquilino para abrir este panel y ver un estado detallado y los pasos siguientes recomendados.

Informes de estado de implementación

Microsoft 365 Lighthouse ahora proporciona un estado de plan de implementación para cada inquilino activo para ayudarle a optimizar y priorizar los esfuerzos de implementación. El estado del plan de implementación se encuentra en la página Inquilinos y en la nueva página Información de implementación.

Febrero de 2023

Información de aplicaciones de Análisis de puntos de conexión

Hemos agregado información de Análisis de puntos de conexión a Microsoft 365 Lighthouse para ayudarle a tomar medidas proactivamente para mejorar el estado de los dispositivos de usuario y las aplicaciones dentro de los inquilinos administrados. La información de Análisis de puntos de conexión informa a una subtarea de implementación denominada **Habilitar supervisión del estado del dispositivo** dentro

de la línea base predeterminada en la tarea **Configurar inscripción de dispositivos**. Una vez habilitada la nueva subtarea e implementada la tarea de implementación, seleccione **Aplicaciones**>**Rendimiento de aplicaciones** en el panel de navegación izquierdo de Microsoft 365 Lighthouse para ver la información de Análisis de puntos de conexión.

Para obtener más información, consulte ¿Qué es Análisis de puntos de conexión?.

Información de dispositivos de Análisis de puntos de conexión

Hemos agregado información de Análisis de puntos de conexión a Microsoft 365 Lighthouse para ayudarle a tomar medidas proactivamente para mejorar el estado de los dispositivos de usuario y las aplicaciones dentro de los inquilinos administrados. La información de Análisis de puntos de conexión informa a una subtarea de implementación denominada **Habilitar supervisión del estado del dispositivo** dentro de la línea base predeterminada en la tarea **Configurar inscripción de dispositivos**. Una vez habilitada la nueva subtarea y implementada la tarea de implementación, seleccione **Dispositivos**>**Estado del dispositivo** en el panel de navegación izquierdo de Microsoft 365 Lighthouse para ver la información de Análisis de puntos de conexión.

Para obtener más información, consulte ¿Qué es Análisis de puntos de conexión?.

Puntuación de exposición y recomendaciones multiinquilino

Hemos incorporado funcionalidades de administración de amenazas y vulnerabilidades multiinquilino de Microsoft Defender para punto de conexión (MDE) a Microsoft 365 Lighthouse. Para ver los niveles de exposición de todos los inquilinos administrados incorporados a MDE, vaya a **Dispositivos**>**Administración de vulnerabilidades** en Microsoft 365 Lighthouse.

Detección de estado de implementación persistente y análisis de desfase de configuración

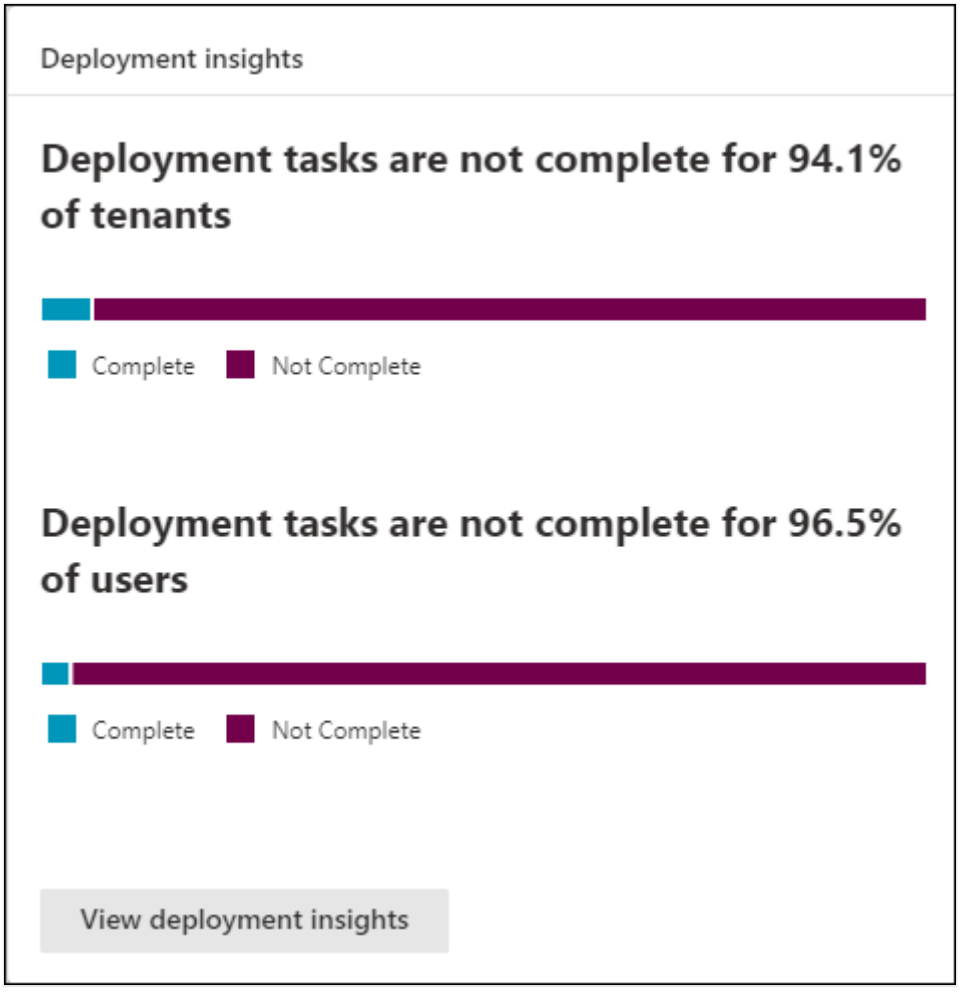
Hemos mejorado Microsoft 365 Lighthouse para proporcionar detección de configuración persistente y estado de implementación para supervisar los inquilinos, incluso cuando está sin conexión, e identificar las actualizaciones de una configuración de inquilino que dan lugar a una regresión del estado de implementación para cualquiera de las tareas asignadas.

Microsoft 365 Lighthouse también proporciona detalles sobre *quién*, *dónde* y *cuándo* se produjo la actividad del usuario que provocó el desfase detectado para que pueda restaurar de forma eficaz y eficiente el inquilino al estado deseado.

Esta información le ayuda a interactuar eficazmente con otros administradores de inquilinos(ya sea en su organización o en la organización del cliente) para educarlos sobre el impacto de su actividad y cómo mitigar los riesgos futuros asociados con el desfase de configuración.

Tarjeta de página principal de Información de implementación

La página principal de Microsoft 365 Lighthouse ahora incluye una tarjeta de información de implementación que proporciona información útil sobre el estado de implementación de los inquilinos que administra. Estas conclusiones pueden ayudar a identificar dónde centrar las actividades de implementación para optimizar el estado y la seguridad de los inquilinos.



Progreso de la implementación por usuario

Microsoft 365 Lighthouse ahora notifica el progreso de la implementación por parte del usuario para que pueda ver el estado de implementación de cada tarea de implementación aplicable. La capacidad de ver cuáles usuarios cumplen, no cumplen, no están destinados, no tienen licencia o se excluyen de cada tarea de implementación en todos los inquilinos administrados pueden ayudarle a contribuir de forma más eficaz y eficiente a cada usuario para ser seguro y productivo.

Enero de 2023

Automatización de la inscripción de dispositivos de Intune mediante la línea base predeterminada

La línea base predeterminada ahora proporciona una subtarea de administración de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM) para automatizar la inscripción de dispositivos Windows en Intune. Anteriormente, se trataba de una tarea manual que solo proporcionaba instrucciones.

Para cualquier inquilino, vaya a la página **Plan de implementación**, expanda la tarea **Configuración de inscripción de dispositivos**, seleccione la subtarea **Configurar inscripción de dispositivos** para abrir el panel de detalles de la tarea y, a continuación, seleccione **Implementar**.

Mejoras en la búsqueda de usuarios

La página **Administración de cuentas**>**Usuarios de búsqueda** ahora muestra los resultados de la búsqueda en cuanto se encuentra un usuario coincidente en cualquier inquilino. La versión anterior de la página mostró resultados de búsqueda solo después de buscar en todos los inquilinos.

Noviembre de 2022

Cambios en las tareas de implementación de Firewall de Microsoft Defender y Antivirus de Microsoft Defender

Hemos actualizado la configuración de directiva de Firewall de Microsoft Defender y Antivirus de Microsoft Defender en nuestra línea base predeterminada para proporcionar protección mejorada para los inquilinos de los clientes. Si anteriormente implementó las tareas **Configuración de Firewall de Microsoft Defender para Windows 10 y versiones posteriores** o **Configuración de Antivirus de Microsoft Defender para**

Windows 10 y versiones posteriores, los inquilinos del cliente siguen protegidos con la configuración de directiva original. Sin embargo, en la página Plan de implementación, los pasos de implementación de estas dos tareas mostrarán el estado **No conforme** hasta que implemente la nueva configuración de directiva mejorada. Para activar esta configuración de directiva mejorada, tendrá que volver a realizar el proceso de implementación para las tareas de implementación de Firewall de Microsoft Defender y Antivirus de Microsoft Defender. Una vez implementados, los estados del paso de implementación se mostrarán como **Conforme** de nuevo.

Funcionalidad para configurar privilegios administrativos delegados pormenorizadas (GDAP)

Ahora puede establecer relaciones de GDAP con varios clientes revendedores a la vez desde Microsoft 365 Lighthouse y asignar usuarios del inquilino del partner a grupos de seguridad con varios roles y niveles de permisos. Para ello, creará plantillas reutilizables basadas en niveles de soporte técnico para los clientes y para varios grupos de técnicos. Verá los roles recomendados para cada nivel de soporte técnico durante este proceso. Una vez creadas, estas plantillas se pueden volver a aplicar según sea necesario para los nuevos clientes. Esta funcionalidad le permite establecer rápidamente GDAP con sus clientes mediante un enfoque con privilegios mínimos para los usuarios como reemplazo de privilegios administrativos delegados (DAP).

Para obtener más información sobre GDAP en Microsoft 365 Lighthouse, consulte Información general sobre los permisos en Microsoft 365 Lighthouse.

Para obtener más información sobre GDAP en todos los servicios, consulte Introducción a los privilegios de administrador delegados pormenorizados (GDAP) - Centro de partners.

Funcionalidad para recopilar diagnósticos de dispositivos Windows

Hemos agregado la funcionalidad para recopilar diagnósticos de dispositivos Windows. Puede acceder a esta característica desde la página Cumplimiento del dispositivo. La acción remota Recopilar diagnósticos le permite recopilar y descargar registros de dispositivos Windows sin interrumpir al usuario.

Administrar buzones compartidos

Ahora puede administrar todos los buzones compartidos y salas de reuniones en los inquilinos administrados en **Usuarios** > **Administración de cuentas** > **Buzones**

compartidos. Desde esta página, puede realizar acciones de administración comunes, como delegar el acceso a otros usuarios y proteger los buzones compartidos bloqueando el acceso directo.

Compatibilidad con la exclusión de archivos en la directiva de antivirus

Ahora puede excluir determinadas amenazas no malintencionadas para que aparezcan para los inquilinos en la página Administración de amenazas de Microsoft 365 Lighthouse. Vaya al plan de implementación del inquilino, seleccione **Configurar una directiva de línea base del Antivirus de Microsoft Defender** y especifique las exclusiones de archivo, carpeta o tipo de archivo.

Estado de implementación

Microsoft 365 Lighthouse ahora proporciona un estado de implementación para el plan de implementación de cada inquilino para que pueda optimizar y priorizar los esfuerzos de implementación en consecuencia.

Información de implementación

Microsoft 365 Lighthouse ahora proporciona información de implementación para ayudarle a comprender la coherencia y eficacia con la que establece y mantiene el estado y la seguridad de los inquilinos que administra. La información proporciona visibilidad específica del inquilino y multiinquilino sobre el progreso de la implementación de cada inquilino, tarea y usuario.

Estas conclusiones le ayudan a:

- Establecer y mantenga una posición de seguridad sólida en toda su cartera.
- Priorizar las actividades de implementación para maximizar la seguridad y minimizar el riesgo.
- Auditar excepciones como los despidos de tareas y las exclusiones de usuarios.

Implementación de línea base mejorada con vínculos directos a configuraciones existentes

Hemos mejorado la experiencia de implementación de línea base para que sea más rápido y fácil garantizar que los inquilinos administrados estén en buen estado y sean seguros. Hemos agregado vínculos a configuraciones de inquilino administradas

detectadas para que pueda encontrar, revisar y modificar fácilmente estas configuraciones de inquilino en el portal de administración aplicable.

Informes de progreso de implementación mejorados

Microsoft 365 Lighthouse ahora proporciona visibilidad sobre el progreso de implementación de cada inquilino administrado desde la página Inquilinos para que pueda ver cuántas de las tareas asignadas son:

- **Conforme**: toda la configuración incluida en la tarea es Conforme.
- **No conforme**: una o varias opciones de configuración incluidas en la tarea están incompletas o son No conformes.
- **Descartada**: se ha descartado la tarea.
- **Sin licencia**: el inquilino no tiene licencia para los servicios necesarios para implementar la configuración asociada a la tarea.

Octubre de 2022

Directivas de protección de aplicaciones

Los proveedores de servicios administrados (MSP) ahora pueden implementar directivas de protección de aplicaciones para sus inquilinos administrados desde la línea base predeterminada en Microsoft 365 Lighthouse, lo que permite una mayor protección de los datos de empresa de los inquilinos. Estas directivas usan Administración de aplicaciones móviles (MAM) en dispositivos iOS y Android para proporcionar la protección más segura para los datos de empresa.

Supervisión del estado del dispositivo

Hemos agregado una nueva subtarea de implementación denominada **Habilitar supervisión del estado del dispositivo** dentro de la línea base predeterminada en la tarea **Configurar inscripción de dispositivos**. Una vez que se habilita la nueva subtarea y se implementa la tarea de implementación, el análisis de puntos de conexión en Microsoft Intune podrá analizar los datos del dispositivo y puede recomendar software, ayudar a mejorar el rendimiento del inicio y corregir problemas comunes de soporte técnico.

Para obtener más información, consulte ¿Qué es Análisis de puntos de conexión?.

Septiembre de 2022

Configuración totalmente automatizada de Microsoft Defender para Empresas

Hemos agregado un paso totalmente automatizado a la línea base predeterminada que le ayuda a configurar los inquilinos de los clientes con Microsoft Defender para Empresas. Este paso aprovisiona automáticamente el inquilino para Microsoft Defender para Empresas e incorpora automáticamente dispositivos inscritos en Intune a Microsoft Defender para Empresas.

Funcionalidad para filtrar la lista de autenticación multifactor (MFA) para mostrar las cuentas de usuario pertinentes

La página de Autenticación multifactor ahora admite el filtrado de la lista de cuentas de usuario por tipo de cuenta (por ejemplo, por administrador, miembro o invitado). También puede excluir otras cuentas de la lista, como cuentas de servicio o cuentas de acceso de emergencia. Para acceder a esta funcionalidad, vaya a **Usuarios**>**Autenticación multifactor**, seleccione un inquilino de la lista para abrir el panel de detalles del inquilino y, a continuación, seleccione la pestaña **Usuarios no registrados para MFA**. Estas funcionalidades de filtrado y exclusión le ayudan a centrarse en las cuentas de usuario pertinentes.

Funcionalidad para actuar sobre incidentes de seguridad y alertas

Ahora puede actuar sobre los incidentes y alertas que se muestran en la página**Seguridad del dispositivo**>**Incidentes y alertas**. Las acciones admitidas actualmente incluyen la asignación del incidente o la alerta a usted mismo o la resolución del incidente o la alerta.

Agosto de 2022

Visualización y administración de cuentas de usuario inactivas

Microsoft 365 Lighthouse ahora proporciona una lista de todas las cuentas de usuario inactivas de los inquilinos administrados. Para acceder a la lista, seleccione **Usuarios**>**Usuarios inactivos** en el panel de navegación izquierdo de Microsoft 365 Lighthouse. Puede reducir los riesgos de seguridad mediante esta lista para realizar un

seguimiento y limpiar las cuentas que todavía están habilitadas, pero que no se han usado en los últimos seis meses.

Implementación de directivas de Microsoft Edge

Hemos agregado una tarea de implementación de directivas de Microsoft Edge a la línea base predeterminada. Esta tarea de implementación le permite proteger los exploradores del inquilino del cliente con la configuración de seguridad de Edge, que incluye protección integrada contra phishing y malware. Microsoft Edge ha demostrado ser más seguro que Google Chromium para pequeñas y medianas empresas con dispositivos que ejecutan Windows 10 o posterior.

Para obtener más información, consulte Seguridad de Microsoft Edge para su empresa.

Julio de 2022

Implementación de línea base mejorada

Microsoft 365 Lighthouse ahora hace que la implementación de líneas base en todos los inquilinos administrados sea más rápida y fácil:

- Detectar e informar automáticamente del estado de cada tarea asignada
- Consolidación de los informes de estado y simplificación de la lógica que determina el estado de implementación
- Informar sobre qué tareas están completas y qué tareas necesitan su atención
- Notificación del estado de implementación de nivel de usuario para las tareas aplicables
- Detección de configuraciones existentes desde el inquilino y comparación con la línea base
- Proporcionar detalles sobre las tareas que se han descartado
- Identificación de dónde se requieren licencias adicionales para completar una tarea asignada

Junio de 2022

Soporte técnico para clientes de Microsoft 365 E5

Hemos cambiado los requisitos de incorporación para permitirle incorporar clientes de Microsoft 365 E5 a Microsoft 365 Lighthouse. La lista ampliada de licencias que Microsoft 365 Lighthouse admite para la incorporación incluye Microsoft 365 Empresa

Premium, Microsoft 365 E3, Microsoft 365 E5, Microsoft Defender para Empresas y Windows 365 para empresas. Los clientes que tengan al menos una de estas licencias, cumplan los requisitos de privilegios de acceso delegado y no superen el número máximo de usuarios con licencia se pueden administrar en Microsoft 365 Lighthouse.

Para obtener una lista completa de los requisitos, consulte Requisitos para obtener Microsoft 365 Lighthouse.

Integración de Microsoft Defender para Empresas

Microsoft 365 Lighthouse ahora se integra con Microsoft Defender para Empresas para proporcionarle información relacionada y funcionalidades de administración para todos los inquilinos de clientes que tienen Microsoft Defender para Empresas. Para ver la lista de dispositivos de cliente que se han incorporado a Microsoft Defender para Empresas, seleccione **Dispositivos** en el panel de navegación izquierdo de Microsoft 365 Lighthouse. Para ver la lista de incidentes y alertas marcados en los inquilinos de los clientes, vaya a **Dispositivos**>**Seguridad de dispositivos**y, a continuación, seleccione la pestaña **Incidentes y alertas**.

También hemos agregado un paso a la línea base predeterminada para ayudarle a configurar Microsoft Defender para Empresas para los inquilinos del cliente. Para ver este paso, seleccione **Líneas base** en el panel de navegación izquierdo de Microsoft 365 Lighthouse o vea el plan de implementación para cualquiera de los inquilinos del cliente.

Estado de los mensajes de correo electrónico en cuarentena

Hemos agregado una nueva funcionalidad en torno a los datos de cuarentena de correo electrónico para los inquilinos administrados. Accesible mediante la selección de **Protección de datos** en el panel de navegación izquierdo de Microsoft 365 Lighthouse, esta característica proporciona visibilidad sobre el estado de los mensajes de correo electrónico en cuarentena en los inquilinos del cliente. Puede ver información consolidada de los volúmenes de cuarentena totales e información detallada de cada inquilino administrado para ayudarle a priorizar los inquilinos que puedan requerir acción.

Aumento del límite máximo de licencias

Estamos haciendo posible administrar más clientes en Microsoft 365 Lighthouse al aumentar de nuevo el límite máximo de licencias para la incorporación de clientes. Los

clientes con hasta 2500 licencias de usuario ahora se pueden incorporar a Microsoft 365 Lighthouse. Seguiremos evaluando este requisito en futuras versiones de Microsoft 365 Lighthouse.

Para obtener más información, consulte Requisitos para Microsoft 365 Lighthouse.

Mayo de 2022

Panel de navegación izquierdo rediseñado

Hemos dado un nuevo aspecto al panel de navegación izquierdo de Microsoft 365 Lighthouse. Observará un diseño más elegante, con nodos de nivel superior como inquilinos, usuarios y dispositivos que se expanden para mostrar subnodos relacionados, como usuarios de riesgo, cumplimiento de dispositivos y administración de amenazas. Este modelo de navegación se alinea con el modelo usado por otros Centros de administración de Microsoft 365.

Panel de detalles del usuario enriquecido

Hemos rediseñado el panel de detalles del usuario para incluir más información del usuario y más acciones que puede realizar para administrar mejor a los usuarios. Ahora tiene el mismo aspecto que el panel de detalles del usuario en el Centro de administración de Microsoft 365. Para acceder al panel de detalles del usuario en Microsoft 365 Lighthouse, seleccione **Usuarios** en el panel de navegación izquierdo y, a continuación, seleccione **Buscar usuarios** o **Usuarios de riesgo**. Seleccione cualquier usuario para abrir el panel de detalles.

Abril de 2022

Tipo de acceso delegado y roles en la página Inquilinos

Hemos actualizado la página **Inquilinos** para mostrar el tipo de acceso delegado del proveedor de servicios administrados (MSP) (Ninguno, DAP, GDAP o Ambos DAP y GDAP) por cliente en la columna **Acceso delegado**. También hemos agregado una nueva columna titulada **Sus roles** que enumera los roles DAP y GDAP por cliente para un usuario que ha iniciado sesión. Estas dos mejoras en la página **Inquilinos** facilitarán a los técnicos de MSP comprender qué tipos de privilegios administrativos delegados están disponibles para cada cliente y qué roles delegados se les han concedido explícitamente.

Para obtener más información, consulte Información general sobre los permisos en Microsoft 365 Lighthouse.

Marzo de 2022

Acciones de integración y administración de Windows 365 Business

En función de los comentarios de los usuarios, hemos integrado Windows 365 Business en Microsoft 365 Lighthouse. Esta integración le ayudará a administrar y supervisar todos los equipos en la nube de sus clientes desde una sola ubicación.

Además de la integración con equipos de Windows 365 Business Cloud en Microsoft 365 Lighthouse, ahora puede realizar las siguientes acciones de administración:

- Restart
- Reaprovisionamiento
- Cambiar nombre

Para obtener más información sobre las nuevas características, consulte Información general de la página Windows 365 (PC en la nube) en Microsoft 365 Lighthouse.

Modificación de partners de Microsoft 365 Lighthouse

Ahora que Microsoft 365 Lighthouse está en disponibilidad general, es necesario que nuestros partners actuales firmen una modificación actualizada de los partners de Lighthouse de Microsoft 365. A todos los partners de Microsoft 365 Lighthouse que se registraron durante el período de versión preliminar se les pedirá que completen este nuevo contrato en las próximas semanas. La finalización requerirá derechos de Administrador global en el inquilino del partner y debe completarse en un plazo de 90 días para seguir accediendo al portal de Microsoft 365 Lighthouse.

Febrero de 2022

Roles de privilegios administrativos delegados granulares (GDAP)

Microsoft 365 Lighthouse ahora incluye la funcionalidad para que los CSP usen roles de privilegios administrativos delegados pormenorizadas (GDAP). Con la actualización más reciente, los MSP pueden aprovechar GDAP mediante la asignación de roles a sus

técnicos para aplicar el principio de acceso con privilegios mínimos en Microsoft 365 Lighthouse. Esta funcionalidad reduce los riesgos inherentes a los amplios permisos del rol de privilegios administrativos delegados (DAP) del agente de Administración habilitando controles pormenorizados sobre los datos y la configuración de los clientes con los que cada técnico podrá trabajar.

Para más información sobre GDAP en Microsoft 365 Lighthouse, consulte Configuración de la seguridad del portal de Microsoft 365 Lighthouse.

Funcionalidad para notificar a los usuarios para que actúen en dispositivos no conformes

Como parte del paso de línea base de cumplimiento de dispositivos, hemos agregado la capacidad de notificar a los usuarios de un inquilino de cliente para que actúen en dispositivos no conformes. Con este cambio, una vez aplicado el paso de implementación de cumplimiento de dispositivos para cualquier inquilino de cliente, la directiva de cumplimiento de dispositivos creada en ese inquilino enviará automáticamente una notificación a los usuarios cuando su dispositivo pase a ser no conforme recordándoles que realicen las acciones adecuadas para que el dispositivo vuelva a ser conforme.

Validación de la implementación e informes

Microsoft 365 Lighthouse ahora puede probar las configuraciones de inquilino para los pasos de implementación con directivas de acceso condicional.

Esta nueva funcionalidad detecta las directivas existentes dentro de los inquilinos del cliente que administra y las compara con el plan de implementación. A continuación, Microsoft 365 Lighthouse proporciona designaciones de estado para los pasos de implementación y los procesos de paso de implementación para ayudarle a comprender qué procesos de implementación ya se han completado, cuáles deben abordarse y dónde la configuración prescrita por el plan de implementación es igual, falta o entra en conflicto con la configuración incluida en las directivas existentes. Conocer esta información hace que la identificación, priorización y resolución de conflictos de directivas sea más rápida, fácil y eficaz.

Paso de implementación para configurar el Firewall de Microsoft Defender

Microsoft 365 Lighthouse ha agregado el paso Configurar la implementación del Firewall de Microsoft Defender a su línea base predeterminada. Este paso ayuda a los

MSP a proteger los dispositivos de inquilino del cliente a través de la configuración de firewall predeterminada para dispositivos Windows 10 (y versiones posteriores). El Firewall de Microsoft Defender bloquea el tráfico de red no autorizado que entra o sale de los dispositivos de inquilino del cliente y reduce el riesgo de amenazas de seguridad de red. Actualmente se está desarrollando una característica de reglas de Firewall de Microsoft Defender.

El firewall de Microsoft Defender está activado de forma predeterminada en dispositivos Windows 10 (y versiones posteriores). Si el inquilino del cliente no tiene esto configurado, siga estos pasos:

1. En la página **Inquilinos** de Microsoft 365 Lighthouse, seleccione el inquilino del cliente para abrir la página **Información general** del inquilino.
2. Seleccione la pestaña **Implementación**.
3. En la lista de pasos de implementación, seleccione **Configurar Firewall de Microsoft Defender**.
4. Seleccione **Revisar e implementar** para implementar esta configuración en el inquilino del cliente.

Aumento del límite máximo de licencias

Estamos haciendo posible administrar más clientes en Microsoft 365 Lighthouse mediante el aumento del límite máximo de licencias para la incorporación de clientes. Los clientes con hasta 1000 licencias de usuario ahora se pueden incorporar a Microsoft 365 Lighthouse. Seguiremos evaluando este requisito en futuras versiones de Microsoft 365 Lighthouse.

Para obtener más información, consulte Requisitos para Microsoft 365 Lighthouse.

Soporte técnico para clientes de asesor

Hemos cambiado los requisitos de incorporación para permitir que los inquilinos de clientes existentes con relaciones de asesor se incorporen a Microsoft 365 Lighthouse. Los clientes con contratos de revendedor y asesor ahora pueden estar en Microsoft 365 Lighthouse si cumplen los requisitos de privilegios de acceso delegado, tienen las licencias necesarias y no superan el número máximo de usuarios.

Para obtener más información, consulte Requisitos para Microsoft 365 Lighthouse.

Enero de 2022

Funcionalidad para ver los registros de auditoría en Microsoft 365 Lighthouse

Microsoft 365 Lighthouse ahora incluye la capacidad de ver los registros de auditoría. Puede revisar las acciones anteriores para encontrar configuraciones incorrectas y acciones de riesgo para la corrección, el proceso de soporte técnico y la investigación de seguridad, entrenar a los empleados y cumplir los requisitos de cumplimiento y auditoría. Con la actualización más reciente, puede hacer lo siguiente:

- Vea los registros de auditoría para ver todas las acciones realizadas dentro de Microsoft 365 Lighthouse, incluido lo que cambió en cuál inquilino del cliente, cuándo se cambió y quién lo cambió.
- Busque y filtre los registros de auditoría para encontrar información específica.
- Exporte los registros para que pueda analizarlos y conservarlos.

En el panel de navegación izquierdo de Microsoft 365 Lighthouse, seleccione **Registros de auditoría**. O bien, vaya directamente a la página Registros de auditoría ahora para comprobarlo.

Noviembre de 2021

Datos de uso de servicios de Microsoft 365

Ahora puede ver los datos de uso de los servicios de Microsoft 365 desde Microsoft 365 Lighthouse. Comprender cómo los clientes usan sus servicios de Microsoft 365 es fundamental para ayudarles a sacar el máximo partido a sus inversiones en TI. En lugar de usar varios recursos para ver información en los distintos servicios de productividad, seguridad y cumplimiento de los clientes, Microsoft 365 Lighthouse los agrega en una vista sencilla y eficaz.

Esta información puede ayudar a informar y ofrecer más valor a los clientes, ya que le permite ayudarles a comprender qué servicios usan activamente sus usuarios y dónde pueden haber oportunidades para mejorar su seguridad o productividad.

Para obtener más información, vea Información general de la página Inquilinos en Microsoft 365 Lighthouse: Uso de aplicaciones y servicios.

Paso de línea de base predeterminado de Exchange Online Protection y Microsoft Defender XDR para Office 365

Hemos agregado un nuevo paso a la línea base predeterminada para incluir instrucciones para habilitar directivas de seguridad para Exchange Online Protection (EOP) y Microsoft Defender para Office 365 (MDO). EOP y MDO ayudan a proteger a los usuarios contra correo no deseado, phishing y correos electrónicos de malware mediante el envío de los correos electrónicos a la carpeta de correo no deseado o cuarentena del usuario (próximamente). El plan de implementación le guía en la configuración de EOP y MDO, ampliando aún más su posición de seguridad durante la siguiente revisión del plan de implementación de inquilinos del cliente.

Etiquetas de inquilino predeterminadas

Ahora puede designar determinadas etiquetas de inquilino *de forma predeterminada* en el panel **Administrar etiquetas** de la página **Inquilinos**, por lo que la próxima vez que inicie sesión en Microsoft 365 Lighthouse, todas las vistas y la información se filtrarán de forma predeterminada para mostrar solo los inquilinos que tienen una etiqueta predeterminada. Las etiquetas predeterminadas pueden ayudarle a centrarse en la información de los inquilinos de clientes de prioridad alta.

Octubre de 2021

Funcionalidad para filtrar por varias etiquetas de inquilino

Ahora es posible filtrar los datos por varias etiquetas de inquilino al mismo tiempo. Esta funcionalidad puede ayudarle a filtrar más fácilmente las vistas e información existentes que están disponibles en Microsoft 365 Lighthouse para mostrar los inquilinos de clientes pertinentes.

Funcionalidad para asignar configuraciones de línea base a grupos específicos de Azure Active Directory

Hemos agregado la capacidad de asignar configuraciones de línea base a grupos específicos de Azure Active Directory (Azure AD) de los inquilinos de los clientes desde Microsoft 365 Lighthouse. En cualquier página de paso de implementación, examine y seleccione los grupos de Azure AD específicos que desea incluir o excluir y, a continuación, implemente las configuraciones en el inquilino del cliente.

Mejoras en página de usuarios de riesgo

Ahora puede ver y comprender fácilmente los motivos del riesgo de un usuario desde Microsoft 365 Lighthouse. En el panel de navegación izquierdo de Microsoft 365 Lighthouse, seleccione **Usuarios** y, a continuación, seleccione la pestaña **Usuarios de riesgo**. Seleccione **Ver detecciones de riesgos** en la columna **Detalles** para cualquier usuario. Desde aquí, puede revisar los detalles del riesgo y, a continuación, seleccionar **Confirmar usuario en peligro** o **Descartar riesgo de usuario**. También puede confirmar o descartar un riesgo para varios usuarios al mismo tiempo desde la página **Usuarios de riesgo**. La capacidad de descartar el riesgo de un usuario puede ser útil cuando el autoservicio de restablecimiento de contraseña (SSPR) no es una opción o si cree que el usuario afectado ya no está en riesgo.

Funcionalidad para proporcionar comentarios sobre Microsoft 365 Lighthouse

Sus comentarios son importantes para nosotros, por lo que hemos agregado una nueva funcionalidad de comentarios que, en ocasiones (no más de una vez al mes), le pedirá que proporcione comentarios. También puede proporcionar comentarios en cualquier momento seleccionando el icono de comentarios en la esquina superior derecha de Microsoft 365 Lighthouse.

Septiembre de 2021

Cambios en el filtro de inquilinos

Hemos realizado algunos cambios en la experiencia de filtrado de inquilinos para ayudarle a ver y administrar rápidamente inquilinos y etiquetas desde cualquier página de Microsoft 365 Lighthouse. Seleccione el filtro **Inquilinos** en la parte superior de cualquier página y, a continuación, examine o escriba el nombre de inquilino o etiqueta por el que desea filtrar.

Agosto de 2021

Flujos de trabajo de correo electrónico del producto para comunicarse con los usuarios

Hemos facilitado la comunicación con los usuarios de los inquilinos del cliente sobre las acciones que deben realizar. En la lista de usuarios no registrados para la autenticación multifactor (MFA) o el autoservicio de restablecimiento de contraseña (SSPR), ahora

puede seleccionar uno o varios usuarios y enviarles un mensaje de correo electrónico mediante una plantilla de correo electrónico descargable.

Funcionalidad para realizar acciones en dispositivos no conformes

Hemos introducido la funcionalidad para sincronizar o reiniciar uno o varios dispositivos en varios inquilinos de clientes. Esta funcionalidad ayuda a garantizar que los dispositivos de los clientes estén protegidos contra riesgos. Para comprobar esta funcionalidad, seleccione **Dispositivos** en el panel de navegación izquierdo de Microsoft 365 Lighthouse y, a continuación, seleccione la pestaña **Dispositivos**. Busque las opciones **Sincronizar** y **Reiniciar** encima de la lista de dispositivos. También puede acceder a estas opciones desde el panel de detalles del dispositivo de cualquier dispositivo.

Funcionalidad para supervisar y administrar equipos en la nube de Windows 365

Hemos agregado la capacidad de supervisar las conexiones locales y aprovisionar y administrar equipos en la nube de Windows 365 en todos los inquilinos del cliente. La nueva página de **Windows 365** proporciona información detallada sobre todos los equipos en la nube de los inquilinos en una ubicación cómoda.

Soporte técnico para clientes de Microsoft 365 E3

Hemos cambiado los requisitos de incorporación para permitirle incorporar clientes de Microsoft 365 E3 a Microsoft 365 Lighthouse. Para poder administrarse en Microsoft 365 Lighthouse, cada cliente debe cumplir los siguientes requisitos:

- Debe tener el acceso delegado configurado para que el MSP pueda administrar el inquilino del cliente
- Debe tener al menos una licencia de Microsoft 365 Empresa Premium o Microsoft 365 E3
- No debe tener más de 500 usuarios con licencia

Para obtener información sobre los requisitos, consulte Requisitos de Microsoft 365 Lighthouse.

Junio de 2021

Funcionalidad para agregar etiquetas personalizadas a inquilinos de clientes

Ahora puede crear y aplicar etiquetas personalizadas a los inquilinos del cliente que administra en Microsoft 365 Lighthouse. Use estas etiquetas para ayudarle a organizar los inquilinos o para filtrar más fácilmente la lista de inquilinos para mostrar información sobre los conjuntos de inquilinos de clientes pertinentes.

Líneas base para estandarizar las implementaciones de inquilinos del cliente

Con la nueva característica de líneas base, ahora puede implementar configuraciones estándar para ayudar a proteger a los usuarios, dispositivos y datos en los inquilinos del cliente. La línea base predeterminada contiene actualmente los siguientes pasos de implementación (con más información próximamente):

- Requerir MFA para administradores
- Requerir MFA para usuarios
- Bloquear la autenticación heredada
- Inscripción de dispositivos Windows en Microsoft Intune: unión a Azure AD
- Configurar la directiva de Antivirus de Defender para dispositivos Windows
- Configuración de la directiva de cumplimiento para dispositivos Windows

Para actuar sobre estos pasos de implementación, seleccione **Inquilinos** en el panel de navegación izquierdo de Microsoft 365 Lighthouse, seleccione un inquilino en la lista de inquilinos y, a continuación, seleccione la pestaña **Plan de implementación**.

Mayo de 2021

Mejoras en la página de Inquilinos

Hemos realizado las siguientes mejoras en la página **Inquilinos** :

- Se ha agregado una lista de recuentos totales por problema a la parte superior de la página.
- Se ha proporcionado la capacidad de mantener el puntero sobre un estado en la columna **Estado** de la lista de inquilinos para ver los detalles de la restricción
- Se han mejorado las etiquetas de estado

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Introducción a Microsoft 365 Lighthouse

Artículo • 11/11/2024

Microsoft 365 Lighthouse ayuda a los proveedores de servicios administrados (MSP) a aumentar su negocio y a ofrecer servicios a los clientes a escala desde un único portal. Con Lighthouse, puede estandarizar configuraciones, administrar riesgos, identificar oportunidades de ventas basadas en inteligencia artificial (IA) e interactuar con los clientes de una manera sin precedentes, lo que le permite anticipar las necesidades de los clientes y maximizar su inversión en Microsoft 365.

En el caso de los CSP con acceso delegado, Lighthouse simplifica la incorporación de inquilinos de clientes al recomendar líneas base de configuración de seguridad adaptadas a los clientes SMB y proporcionar vistas multiinquilino en todos los entornos de cliente. Con Lighthouse, los ingenieros de servicio pueden escalar la administración de sus clientes, centrarse en lo más importante, buscar e investigar rápidamente los riesgos y tomar medidas para que sus clientes se encuentren en un estado seguro y correcto.

Lighthouse también proporciona funcionalidades para los administradores de cuentas. Con información basada en inteligencia artificial, Lighthouse ofrece recomendaciones proactivas, accionables y personalizadas para ayudar a adquirir nuevos clientes, mejorar la retención de clientes y expandir el negocio con ofertas premium.

No hay costos adicionales asociados con el uso de Lighthouse para administrar los servicios de Microsoft 365 y los dispositivos conectados. Lighthouse está disponible para los asociados inscritos en el programa Proveedor de soluciones en la nube (CSP), incluidos Direct-Bill y revendedores indirectos.

> **ⓘ Importante**
>
> Para usar Lighthouse, los MSP y sus inquilinos de cliente deben cumplir los requisitos enumerados en **Microsoft 365 Lighthouse requisitos**.

Para obtener más información sobre el programa CSP, consulte información general sobre el programa Proveedor de soluciones en la nube: Centro de partners.

> **ⓘ Nota**

Una oferta similar, Azure Lighthouse, ayuda a los proveedores de servicios a ofrecer servicios administrados para los servicios de Azure mediante herramientas de administración completas y sólidas integradas en la plataforma Azure. Para más información, consulte **¿Qué es Azure Lighthouse?**

Vea: ¿Qué es Microsoft 365 Lighthouse?

https://learn-video.azurefd.net/vod/player?id=709ebb5a-34ea-417d-8a1e-f105f43feb91&locale=es-es&embedUrl=%2Fmicrosoft-365%2Flighthouse%2Fm365-lighthouse-overview

ventajas Microsoft 365 Lighthouse

Lighthouse ayuda a los MSP a aumentar la seguridad y administrar los servicios de Microsoft 365 y los puntos de conexión conectados a escala mediante:

- Presentar recomendaciones basadas en inteligencia artificial para adquirir y conservar mejor los clientes y hacer crecer su negocio.
- Proporcionar recorridos de implementación de inquilinos para que los técnicos puedan seguir un conjunto coherente de pasos para proteger y configurar los inquilinos del cliente.
- Usar una línea de base de seguridad SMB predeterminada que recete los procedimientos recomendados destinados a inquilinos de pequeñas y medianas empresas.
- Proporcionar información multiinquilino sobre el cumplimiento de dispositivos para obtener una visión clara de cómo se evalúan los dispositivos en todas las organizaciones, las herramientas para comparar las directivas y la configuración superior que no se cumplen.
- Simplificación de tareas comunes, como restablecer una contraseña.
- Configuración de la autenticación multifactor y el autoservicio de restablecimiento de contraseña (SSPR), incluidas herramientas para ayudar a impulsar la adopción por parte de los usuarios.
- Descripción y protección frente a inicios de sesión de riesgo.
- Administrar amenazas en dispositivos Windows 10 proporcionando detalles sobre las amenazas detectadas por Microsoft Defender XDR y las acciones que se deben realizar para resolver problemas y mantener los dispositivos actualizados.
- Proporcionar información sobre los incidentes de servicio de Microsoft 365 y los avisos que afectan a los inquilinos del cliente que administran.

Vea: Demostración de Microsoft 365 Lighthouse

https://learn-video.azurefd.net/vod/player?id=797a2bb2-0ccb-41ac-ac97-80ced13be066&locale=es-es&embedUrl=%2Fmicrosoft-365%2Flighthouse%2Fm365-lighthouse-overview

> **Nota**
>
> Para obtener más información sobre cómo registrarse, consulte **Registrarse para Microsoft 365 Lighthouse**.

Echa un vistazo a los demás vídeos de Microsoft 365 Lighthouse en nuestro canal de YouTube.

Contenido relacionado

Registrarse para obtener Microsoft 365 Lighthouse (artículo)
Información general de la página Inquilinos de Microsoft 365 Lighthouse (artículo)
Información general de la página Cumplimiento de dispositivos en Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)
Microsoft Defender para Empresas (página de vínculo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Requisitos para Microsoft 365 Lighthouse

Artículo • 20/01/2025

Microsoft 365 Lighthouse es un portal de administración que proporciona funcionalidades avanzadas para que los proveedores de servicios administrados (MSP) administren clientes a escala a través de la administración proactiva de cuentas, la incorporación simplificada, la configuración eficaz de inquilinos, la protección de dispositivos y las alertas. Lighthouse proporciona información sobre las oportunidades de adquisición, retención y crecimiento de clientes, así como vistas multiinquilino entre dispositivos de clientes, datos y usuarios para ayudar a los clientes a obtener el máximo valor de Microsoft 365.

Lighthouse está disponible para los asociados inscritos en el programa Proveedor de soluciones en la nube (CSP), incluidos los revendedores indirectos y los asociados de factura directa.

> ⓘ **Nota**
>
> Solo los asociados deben inscribirse en el programa CSP; los clientes que administran no necesitan inscribirse en el programa CSP.

Además, cada inquilino de cliente debe cumplir los siguientes requisitos para supervisarse y administrarse activamente en Lighthouse:

- Debe tener el acceso delegado configurado para que el asociado pueda administrar el inquilino del cliente.

  > ⓘ **Nota**
  >
  > Se requiere privilegios administrativos delegados granulares (GDAP) o una relación de privilegios administrativos delegados (DAP) para incorporar clientes a Lighthouse. Ya no se requiere una relación de revendedor indirecto para incorporarse a Lighthouse. Si DAP y GDAP coexisten en un inquilino de cliente, los permisos de GDAP tienen prioridad para los técnicos de MSP en grupos de seguridad habilitados para GDAP.

  > ⓘ **Nota**

> Para usar Lighthouse para ver oportunidades en Sales Advisor, no necesita permisos de acceso delegado adicionales del cliente.

- Debe tener al menos una suscripción Enterprise, Business, Frontline o Education de Microsoft 365, Office 365, Exchange Online, Windows 365 Business o Microsoft Defender para Empresas
- No debe tener más de 2500 usuarios con licencia
- Debe residir en la misma región geográfica (América, Unión Europea o Asia más Australia) que la organización asociada que los administra.

Los inquilinos del cliente que no cumplan estos requisitos tendrán acceso solo a un conjunto limitado de experiencias en Lighthouse, incluida la configuración y administración de GDAP, la búsqueda de usuarios, los detalles del usuario, el etiquetado de inquilinos y el estado del servicio.

Requisitos para habilitar la administración de dispositivos

Para ver los dispositivos de inquilino del cliente en las páginas de administración de dispositivos, un MSP debe:

- Inscriba todos los dispositivos de cliente en Microsoft Intune. Para obtener más información, consulte Inscripción de dispositivos en Microsoft Intune.
- Asigne directivas de cumplimiento a todos los dispositivos de cliente. Para obtener más información, vea Crear una directiva de cumplimiento en Microsoft Intune.

Requisitos para habilitar la administración de usuarios

Para que los datos de los clientes se muestren en los informes de las páginas de administración de usuarios, incluidos los usuarios de riesgo, la autenticación multifactor y el autoservicio de restablecimiento de contraseña, los inquilinos del cliente deben tener licencias para Azure Active Directory Premium P1 o posterior. Azure AD Premium P1 incluye Microsoft 365 Empresa Premium y Microsoft 365 E3. Azure AD Premium P2 se incluye con Microsoft 365 E5.

Requisitos para habilitar la administración de amenazas

Para ver las amenazas y los dispositivos de inquilino del cliente en las páginas de administración de amenazas, debe inscribir todos los dispositivos de inquilino del cliente en Microsoft Intune y protegerlos mediante la ejecución de Microsoft Defender Antivirus.

Para obtener más información, consulte Inscripción de dispositivos en Microsoft Intune.

Microsoft Defender Antivirus forma parte del sistema operativo Windows y está habilitado de forma predeterminada en dispositivos que ejecutan Windows 10.

> **Nota**
>
> Si usa una solución antivirus que no es de Microsoft y no Microsoft Defender Antivirus, Microsoft Defender Antivirus se deshabilita automáticamente. Al desinstalar la solución antivirus que no es de Microsoft, Microsoft Defender Antivirus se activa automáticamente para proteger los dispositivos Windows frente a amenazas.

Requisitos para habilitar Sales Advisor

Para usar Sales Advisor para ver las oportunidades de los clientes, debe tener el rol Administrador de cuentas en Lighthouse. Si no tiene el rol Administrador de cuentas, póngase en contacto con alguien que tenga el rol Administrador en Lighthouse y pídale que le asigne el rol.

Para obtener más información, consulte Introducción a los permisos en Microsoft 365 Lighthouse.

Contenido relacionado

Configuración de la seguridad del portal de Microsoft 365 Lighthouse (artículo)
Información general de la página Cumplimiento de dispositivos en Microsoft 365 Lighthouse (artículo)
Información general de la página Usuarios de Microsoft 365 Lighthouse (artículo)
Información general de la página Administración de amenazas en Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Regístrese para obtener Microsoft 365 Lighthouse

Artículo • 31/08/2024

En este artículo se proporcionan instrucciones sobre cómo registrarse para Microsoft 365 Lighthouse. Microsoft 365 Lighthouse es un portal de administración que proporciona funcionalidades avanzadas para que los proveedores de servicios administrados (MSP) administren clientes a escala a través de la administración proactiva de cuentas, la incorporación simplificada, la configuración eficaz de inquilinos, la protección de dispositivos y las alertas. Lighthouse proporciona información sobre las oportunidades de adquisición, retención y crecimiento de clientes, así como vistas multiinquilino entre dispositivos de clientes, datos y usuarios para ayudar a los clientes a obtener el máximo valor de Microsoft 365.

Antes de empezar

Microsoft 365 Lighthouse solo se implementa en el inquilino del asociado, no en los inquilinos del cliente, pero asegúrese de que usted y sus inquilinos cumplen los requisitos enumerados en Microsoft 365 Lighthouse requisitos.

Regístrese para obtener Microsoft 365 Lighthouse

1. Ve a https://lighthouse.microsoft.com .

   Si el inquilino del asociado es apto para usar Microsoft 365 Lighthouse, verá un mensaje de bienvenida y los inquilinos administrados comenzarán a cargarse. Una vez completado este proceso de carga inicial (que puede tardar un par de minutos), puede empezar a usar Lighthouse para administrar los clientes.

   > **Nota**
   >
   > Si ve el mensaje "Debe ser revendedor indirecto o asociado de factura directa para usar este servicio", consulte Requisitos para Microsoft 365 Lighthouse para obtener detalles de idoneidad.

2. Si ve el mensaje "Debe registrarse para Microsoft 365 Lighthouse en el Centro de administración de Microsoft 365", póngase en contacto con un administrador del

inquilino del asociado y pídale que siga estos pasos:

a. Vaya a la Centro de administración de Microsoft 365 en https://admin.microsoft.com e inicie sesión con sus credenciales de inquilino de asociado.

b. En el panel de navegación izquierdo, seleccione**Servicios de compra**>**de facturación**>**Microsoft 365**.

> ⓘ Nota
>
> En lugar de **Facturación**, es posible que algunos asociados tengan que **ir a**>**Marketplace Todos los productos** y, a continuación, buscar **Microsoft 365 Lighthouse**.

c. En **Microsoft 365 Lighthouse**, seleccione **Detalles**.

d. Seleccione **Comprar**.

> ⓘ Nota
>
> Lighthouse solo requiere una licencia para el inquilino del asociado. No se requieren licencias adicionales por usuario para el asociado y no se requieren licencias de Lighthouse en ningún inquilino del cliente.

Para comprobar que Lighthouse se agregó correctamente al inquilino, busque Microsoft 365 Lighthouse en **Facturación**>**de sus productos** en el Centro de administración de Microsoft 365.

e. Si no se le redirige al portal de Lighthouse, vaya a https://lighthouse.microsoft.com .

3. Si ve el mensaje "Microsoft 365 Lighthouse se quitó para su organización", significa que la configuración del inquilino del asociado debe modificarse para permitir el uso de Lighthouse. Póngase en contacto con un administrador del inquilino del asociado y pídale que siga estos pasos:

a. Vaya a la Centro de administración de Microsoft 365 en https://admin.microsoft.com e inicie sesión con sus credenciales de inquilino de asociado.

b. En el panel de navegación izquierdo, seleccione **Configuración** **Configuración**>**de la organización**.

c. En la pestaña **Servicios**, seleccione **Microsoft 365 Lighthouse** en la lista de servicios y, a continuación, seleccione la opción para permitir el uso de Microsoft 365 Lighthouse experiencias de administración de clientes en el inquilino.

d. Haga clic en **Guardar**.

> ⓘ **Nota**
>
> Después de completar el registro, los datos del cliente pueden tardar hasta 48 horas en aparecer en Lighthouse.

Pasos siguientes

Lighthouse incluye funcionalidades necesarias y opcionales para ayudarle a configurar la seguridad del portal de Lighthouse. Para obtener más información, consulte Configuración de la seguridad del portal de Microsoft 365 Lighthouse.

Para acceder a la característica Sales Advisor en Lighthouse, debe configurar roles adicionales en el Centro de partners. Para obtener más información, consulte Obtención de acceso a Sales Advisor.

Contenido relacionado

Información general de Microsoft 365 Lighthouse (artículo)
Información general de Sales Advisor (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)
Microsoft 365 Lighthouse y Microsoft Defender para Empresas (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Introducción a los permisos en Microsoft 365 Lighthouse

Artículo • 19/11/2024

los permisos de Microsoft 365 Lighthouse se administran principalmente mediante lo siguiente:

- Control de acceso basado en rol (RBAC) de Lighthouse en el inquilino del asociado
- Privilegios administrativos delegados granulares (GDAP) en el inquilino del cliente

Para usar Lighthouse, necesita una combinación de roles asignados a través de RBAC y GDAP.

Administración de permisos de RBAC de Lighthouse en el inquilino del asociado

Los permisos de Lighthouse en el inquilino del asociado se administran mediante la asignación de roles de RBAC en Lighthouse. Cada rol tiene un conjunto de permisos que determina a qué usuarios de datos pueden acceder y cambiar dentro del inquilino del asociado. Los roles RBAC de Lighthouse no proporcionan acceso a los datos del cliente. El acceso a los datos del cliente se rige por los permisos de GDAP de un usuario de Lighthouse (consulte Administración de GDAP en el inquilino del cliente).

Los roles de RBAC se administran desde la página **de permisos de Lighthouse** en Lighthouse. Para acceder a la página **permisos de Lighthouse** y administrar permisos, debe tener uno de los siguientes roles:

- Administrador de roles con privilegios en Microsoft Entra ID
- Administrador en Lighthouse

Para más información, consulte Administración de permisos de RBAC de Lighthouse en Microsoft 365 Lighthouse.

En la tabla siguiente se proporciona información general sobre cada rol RBAC de Lighthouse. Para obtener una lista de las acciones que cada rol puede realizar en el inquilino del asociado, consulte Funciones y roles de RBAC de Lighthouse.

Expandir tabla

Rol RBAC de Lighthouse	Información general
Administrador de cuentas	Los administradores de cuentas tienen acceso total a las páginas y los datos de Sales Advisor en todo el inquilino del asociado. Los administradores de cuentas pueden exportar datos de Sales Advisor.

Rol RBAC de Lighthouse	Información general
Administrador	Los administradores tienen permisos administrativos completos en Lighthouse. Los administradores pueden administrar permisos de RBAC y GDAP, ver registros de auditoría y crear líneas base, etiquetas y alertas. A los administradores se les asignan automáticamente los roles Administrador de roles con privilegios, Administrador de usuarios y Administrador de grupos en Microsoft Entra ID y el rol Agente de Administración en el Centro de partners.
Autor	Los autores pueden administrar inquilinos, etiquetas, reglas de alerta y líneas base para implementar configuraciones de inquilino.
Operador	Los operadores administran los inquilinos de clientes en Lighthouse en función de los permisos de GDAP asignados para cada inquilino de cliente que administran. Los operadores pueden ver el estado de inquilino del cliente de alto nivel y administrar alertas. A los usuarios de Lighthouse que tengan al menos un rol de Microsoft Entra se les asigna automáticamente el rol Operador. **Nota:** Los administradores de Lighthouse pueden usar plantillas en la página **Acceso delegado** para asignar permisos GDAP a los usuarios de Lighthouse.
Lector	Los lectores tienen acceso de solo lectura a los datos de Lighthouse. Los lectores de Lighthouse pueden ver el estado y las alertas del inquilino del cliente de alto nivel.

Funciones y funcionalidades de RBAC de Lighthouse

En la tabla siguiente se describen las acciones que cada rol RBAC de Lighthouse puede realizar en Lighthouse. Para algunas acciones, debe tener un rol de Microsoft Entra además de un rol RBAC de Lighthouse. Para otras acciones, solo se requiere un rol de Microsoft Entra. Microsoft Entra requisitos de rol se indican en la última columna de la tabla. Para obtener una lista completa de los roles Microsoft Entra y las acciones que pueden realizar, consulte Microsoft Entra roles integrados.

Expandir tabla

Área	Acciones	Administrador de cuentas	Administrador	Autor	Operador	Lector	¿Necesita Microsoft Entra rol?
Página principal	Visualización de datos en tarjetas						Yes
	Agregar usuarios						Yes
	Restablecer contraseña						Yes
	Usuarios fuera del panel						Yes
Alertas	Visualización de alertas y reglas de alertas	✓	✓	✓		✓	No
	Administrar alertas (cambiar gravedad, estado o asignación)		✓	✓			No
	Creación, edición y eliminación de reglas de alerta		✓	✓			No
Conclusiones de Copilot	Visualización de oportunidades y datos de adopción						Yes
Inquilinos	Ver la página **Inquilinos**	✓	✓	✓	✓	✓	No
	Visualización de los detalles del inquilino						Yes
	Exportar datos	✓	✓	✓	✓	✓	No
	Ver etiquetas	✓	✓	✓	✓	✓	No
	Creación, actualización y eliminación de etiquetas en Lighthouse		✓	✓			No
	Asignación y eliminación de etiquetas de inquilinos		✓	✓			No

Área	Acciones	Administrador de cuentas	Administrador	Autor	Operador	Lector	¿Necesita Microsoft Entra rol?
	Activación e inactivación de un inquilino		✓	✓			No
	Visualización del estado de acceso delegado	✓	✓	✓	✓	✓	No
	Visualización de la puntuación segura de Microsoft						Yes
	Visualización de asignaciones de línea base	✓	✓	✓	✓	✓	No
	Visualización del estado de la implementación				✓		Yes
	Visualización del uso de aplicaciones y servicios				✓		Yes
	Visualización y edición de la información de contactos y sitios web del cliente	✓	✓		✓	✓	No
Usuarios	Búsqueda de usuarios						Yes
	Visualización de métricas de usuario						Yes
	Incorporación de nuevos usuarios						Yes
	Usuarios fuera del panel						Yes
	Visualización de usuarios inactivos						Yes
	Visualización de buzones compartidos						Yes

Área	Acciones	Administrador de cuentas	Administrador	Autor	Operador	Lector	¿Necesita Microsoft Entra rol?
	Visualización y administración de usuarios de riesgo						Yes
	Visualización y administración de la autenticación multifactor						Yes
	Visualización y administración del autoservicio de restablecimiento de contraseña						Sí
Dispositivos	Visualización de datos de seguridad de dispositivos						Yes
	Visualización de datos de administración de vulnerabilidades						Yes
	Visualización de datos de cumplimiento de dispositivos						Yes
	Visualización de datos de administración de amenazas						Yes
	Visualización de datos de estado del dispositivo						Yes
	Visualización de datos Windows 365						Yes
	Visualización de registros de eventos de Windows						Yes

Área	Acciones	Administrador de cuentas	Administrador	Autor	Operador	Lector	¿Necesita Microsoft Entra rol?
Aplicaciones	Visualización del rendimiento de la aplicación y los datos de administración de aplicaciones						Yes
Mensajes en cuarentena	Visualización y administración de mensajes en cuarentena						Yes
Líneas base	Visualización de líneas base (predeterminadas, personalizadas) y detalles de tareas		✓	✓	✓	✓	No
	Creación, clonación, edición y asignación de líneas base		✓	✓			No
	Extracción de una tarea de un inquilino para agregarla a una línea base		✓	✓			Yes
	Visualización de información de implementación						Yes
Estado del servicio	Supervisión del estado[del servicio 1]						No
Soporte técnico	Creación y administración de solicitudes de servicio[2]						No
Registros de auditoría	Visualización de registros de auditoría		✓				Yes
Permisos	Ver la página **Permisos de Lighthouse**		✓				No
	Configuración y administración de		✓				No

Área	Acciones	Administrador de cuentas	Administrador	Autor	Operador	Lector	¿Necesita Microsoft Entra rol?
	permisos de Lighthouse						
	Visualización, configuración y administración de GDAP en la página **Acceso delegado**		✓				No
Asesor de ventas	Visualización de oportunidades	✓	✓				No
	Visualización de las renovaciones de suscripciones	✓	✓				No
	Visualización de solicitudes de licencia	✓	✓				No

[1] Para supervisar el estado del servicio, los usuarios de Lighthouse deben tener al menos un rol Microsoft Entra en el inquilino del asociado con el siguiente conjunto de propiedades: **microsoft.office365.serviceHealth/allEntities/allTasks**. Los usuarios también deben tener al menos el rol agente de Administración o el rol Agente del departamento de soporte técnico asignados en el Centro de partners.

[2] Para crear y administrar solicitudes de servicio, los usuarios de Lighthouse deben tener al menos un rol de Microsoft Entra en el inquilino del asociado con el siguiente conjunto de propiedades: **microsoft.office365.supportTickets/allEntities/allTasks**.

Administración de GDAP en el inquilino del cliente

Al igual que los roles RBAC de Lighthouse administran permisos en el inquilino del asociado, GDAP administra los permisos en los inquilinos del cliente. GDAP proporciona un alto nivel de control y flexibilidad al proporcionar acceso a los inquilinos del cliente a través de Microsoft Entra roles integrados. La asignación de los roles con privilegios mínimos por tarea a los técnicos de MSP a través de GDAP reduce el riesgo de seguridad para los MSP y los clientes. Se recomienda usar roles de lector GDAP entre inquilinos de clientes para proporcionar a los usuarios de Lighthouse una vista agregada en todos los inquilinos de clientes.

Para obtener más información sobre cómo configurar una relación GDAP con un inquilino de cliente en Lighthouse, consulte Obtención de permisos de administrador pormenorizados para

administrar el servicio de un cliente: Centro de partners.

Para obtener más información sobre los roles con privilegios mínimos por tarea, vea Roles con privilegios mínimos: roles del Centro de partners y roles con privilegios mínimos por tarea en Microsoft Entra ID.

Para obtener más información sobre el desuso de GDAP o los privilegios administrativos delegados (DAP), consulte Preguntas más frecuentes sobre GDAP: Centro de partners o busque fechas y escalas de tiempo en los anuncios del Centro de partners.

Para obtener una lista completa de los roles Microsoft Entra y las acciones que pueden realizar, consulte Microsoft Entra roles integrados. Para obtener información sobre cómo asignar roles, consulte Asignación de roles Microsoft Entra a los usuarios.

Contenido relacionado

Ver los roles de Microsoft Entra en Microsoft 365 Lighthouse (artículo)
Administración de permisos de RBAC de Lighthouse en Microsoft 365 Lighthouse (artículo)
Configuración de GDAP en Microsoft 365 Lighthouse (artículo)
Información general de la página Acceso delegado en Microsoft 365 Lighthouse (artículo)
Asignación de roles y permisos a los usuarios: Centro de partners (artículo)
Preguntas más frecuentes sobre GDAP: Centro de partners (artículo)
Microsoft 365 Lighthouse preguntas más frecuentes (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Administración de permisos de control de acceso basado en rol (RBAC) de Lighthouse en Microsoft 365 Lighthouse

Artículo • 02/11/2024

La página **Permisos de Lighthouse** permite a los administradores de Microsoft 365 Lighthouse administrar permisos de control de acceso basado en rol (RBAC) de usuario en el inquilino del asociado. Los administradores de Lighthouse pueden ver y administrar la pertenencia a cada rol RBAC de Lighthouse para asegurarse de que los usuarios del inquilino asociado tienen permisos de tamaño correcto. Cada rol RBAC de Lighthouse está asociado a un grupo de seguridad en lugar de a un rol de Microsoft Entra, por lo que cuando a los usuarios se les asigna un rol RBAC de Lighthouse, se asocian automáticamente a un grupo de seguridad de RBAC de Lighthouse específico.

> ⓘ **Nota**
>
> Los roles RBAC de Lighthouse no proporcionan acceso a los datos del cliente. El acceso a los datos del cliente se rige por los permisos de GDAP de un usuario de Lighthouse. Para más información, consulte Administración de GDAP en el inquilino del cliente.

Cuando los administradores asignan un rol RBAC de Lighthouse a un usuario del inquilino del asociado por primera vez, se crea automáticamente un grupo de seguridad. Los administradores de Lighthouse pueden ver el grupo de seguridad asociado para cada rol RBAC de Lighthouse en la página **permisos de Lighthouse** y en el Centro de administración Microsoft Entra. Todos los cambios de pertenencia a grupos de seguridad se reflejan tanto en Lighthouse como en la Centro de administración Microsoft Entra.

Antes de empezar

Para acceder a la página **permisos de Lighthouse** y administrar permisos, debe ser administrador en Lighthouse o administrador de roles con privilegios en Microsoft Entra ID.

Visualización de la pertenencia a roles RBAC de Lighthouse y el grupo de seguridad asociado

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Permisos permisos>de Lighthouse**.
2. Seleccione un rol de Lighthouse en la lista para abrir el panel de detalles del rol de Lighthouse.
3. Vea los usuarios del inquilino asociado a los que se les asigna el rol RBAC de Lighthouse y el grupo de seguridad asociado.

> **Nota**
>
> Para ver la pertenencia a grupos de seguridad de los usuarios de Lighthouse con el rol Operador de Lighthouse, vaya a la página **Acceso delegado** de Lighthouse. La página **Acceso delegado** proporciona detalles de pertenencia a grupos de seguridad para todas las relaciones de acceso delegado.

Asignación de roles RBAC de Lighthouse a los usuarios del inquilino del asociado

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Permisos permisos>de Lighthouse**.
2. Seleccione un rol de Lighthouse en la lista para abrir el panel de detalles del rol de Lighthouse.
3. Seleccione **Asignar usuarios**.
4. Seleccione los usuarios que desea asignar al rol RBAC de Lighthouse.
5. Seleccione **Asignar usuarios**.

> **Nota**
>
> El rol Operador de Lighthouse se puede ver, pero no se puede asignar desde la página **Permisos de Lighthouse** . El rol Operador de Lighthouse se asigna automáticamente a los usuarios de Lighthouse que tienen al menos un rol de Microsoft Entra.

Eliminación de usuarios del inquilino del asociado de un rol RBAC de Lighthouse

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Permisos permisos>de Lighthouse**.
2. Seleccione un rol de Lighthouse en la lista para abrir el panel de detalles del rol de Lighthouse.
3. Realiza una de las siguientes acciones:
    - Para quitar un único usuario del rol RBAC de Lighthouse, seleccione la **X** junto al usuario que desea quitar.
    - Para quitar varios usuarios del rol RBAC de Lighthouse, seleccione los usuarios que desea quitar y, a continuación, seleccione **Quitar usuarios**.
4. En la ventana de confirmación, seleccione **Quitar usuarios** para confirmar la eliminación.

Creación o actualización de un grupo de seguridad para un rol RBAC de Lighthouse

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Permisos permisos>de Lighthouse**.
2. Seleccione un rol de Lighthouse en la lista para abrir el panel de detalles del rol de Lighthouse.
3. Seleccione **Actualizar grupo de seguridad**.
4. Realiza una de las siguientes acciones:
    - Seleccione **Usar un grupo de seguridad existente**, seleccione un grupo de seguridad de la lista y, a continuación, seleccione **Guardar**.
    - Seleccione **Crear un nuevo grupo de seguridad**, escriba un nombre para el nuevo grupo, escriba opcionalmente una descripción y agregue usuarios y, a continuación, seleccione **Guardar**.

> ⓘ **Nota**
>
> Debe asignar el rol de administrador de Lighthouse a un grupo de seguridad asignable a roles. Además, para poder asignar roles a un grupo de seguridad

asignable a roles o crear grupos de seguridad asignables por roles, debe tener una licencia Microsoft Entra ID P1. Para habilitar roles Just-In-Time (JIT), se requiere Microsoft Entra gobernanza del IDE o una licencia de Microsoft Entra ID P2.

Puede asignar todos los demás roles de RBAC de Lighthouse a cualquier grupo de seguridad, ya sea asignable o no a roles, pero tenga en cuenta el requisito de licencia P1 para los grupos de seguridad asignables por roles.

Para más información, consulte Uso de grupos de Microsoft Entra para administrar las asignaciones de roles.

Pasos siguientes

Después de agregar o quitar usuarios a los roles de RBAC de Lighthouse disponibles, vaya a la página **permisos de Lighthouse** para ver la pertenencia al grupo más reciente para cada rol.

> **Nota**
>
> Una vez que agregue o quite un usuario a un rol RBAC de Lighthouse, los cambios de pertenencia a grupos pueden tardar hasta una hora en aparecer en Lighthouse.

Para obtener más información sobre cada rol RBAC de Lighthouse para determinar qué roles deben tener los usuarios en el inquilino del asociado, consulte Introducción a los permisos en Microsoft 365 Lighthouse.

Contenido relacionado

Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Administración de permisos de RBAC de Lighthouse en Microsoft 365 Lighthouse (artículo)
Ver los roles de Microsoft Entra en Microsoft 365 Lighthouse (artículo)
Uso de grupos de Microsoft Entra para administrar las asignaciones de roles (artículo)
Microsoft 365 Lighthouse preguntas más frecuentes (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Configuración de la seguridad del portal de Microsoft 365 Lighthouse

Artículo • 31/10/2024

Proteger el acceso a los datos del cliente cuando un proveedor de servicios administrados (MSP) tiene permisos de acceso delegados a sus inquilinos es una prioridad de ciberseguridad. Microsoft 365 Lighthouse incluye funcionalidades necesarias y opcionales para ayudarle a configurar la seguridad del portal de Lighthouse. Debe configurar roles específicos con la autenticación multifactor (MFA) habilitada para poder acceder a Lighthouse. Opcionalmente, puede configurar Microsoft Entra Privileged Identity Management (PIM) y acceso condicional.

Configuración de la autenticación multifactor (MFA)

Como se mencionó en la entrada de blog Your Pa$$word doesn't matter :

> "La contraseña no importa, pero MFA sí. Según nuestros estudios, su cuenta tiene más de un 99,9 % menos de probabilidades de verse comprometida si usa MFA".

Cuando los usuarios accedan a Lighthouse por primera vez, se les pedirá que configuren MFA si su cuenta de Microsoft 365 aún no la tiene configurada. Los usuarios no podrán acceder a Lighthouse hasta que se complete el paso de configuración de MFA necesario. Para más información sobre los métodos de autenticación, consulte Configuración del inicio de sesión de Microsoft 365 para la autenticación multifactor .

Configuración del control de acceso basado en rol

El control de acceso basado en rol (RBAC) concede acceso a recursos o información en función de los roles de usuario. El acceso a los datos y la configuración del inquilino del cliente en Lighthouse está restringido a roles específicos del programa Proveedor de soluciones en la nube (CSP). Para configurar roles de RBAC en Lighthouse, se recomienda usar privilegios administrativos delegados granulares (GDAP) para implementar asignaciones pormenorizadas para los usuarios. Los privilegios administrativos delegados (DAP) siguen siendo necesarios para que el inquilino se incorpore correctamente, pero los clientes solo de GDAP pronto podrán incorporarse sin

dependencias de DAP. Los permisos GDAP tienen prioridad cuando DAP y GDAP coexisten para un cliente.

Para configurar una relación GDAP, consulte Obtención de permisos de administrador granulares para administrar el servicio de un cliente: Centro de partners. Para obtener más información sobre qué roles se recomiendan usar Lighthouse, consulte Información general sobre los permisos en Microsoft 365 Lighthouse.

Los técnicos de MSP también pueden acceder a Lighthouse mediante Administración roles de agente o agente del departamento de soporte técnico a través de privilegios administrativos delegados (DAP).

Para las acciones relacionadas con inquilinos que no son del cliente en Lighthouse (por ejemplo, incorporación, desactivación o reactivación del cliente, administración de etiquetas, revisión de registros), los técnicos de MSP deben tener un rol asignado en el inquilino del asociado. Consulte Introducción a los permisos en Microsoft 365 Lighthouse para obtener más información sobre los roles de inquilino de asociados.

Configuración de Microsoft Entra Privileged Identity Management (PIM)

Los CSP pueden minimizar el número de personas que tienen acceso a roles con privilegios elevados para proteger la información o los recursos mediante PIM. PIM reduce la posibilidad de que una persona malintencionada obtenga acceso a los recursos o a los usuarios autorizados que afecten involuntariamente a un recurso confidencial. Los CSP también pueden conceder a los usuarios roles de privilegios elevados Just-In-Time para acceder a los recursos, realizar cambios amplios y supervisar lo que hacen los usuarios designados con su acceso con privilegios.

> ⓘ **Nota**
>
> El uso de Microsoft Entra PIM requiere una licencia Microsoft Entra ID P2 en el inquilino del asociado.

Los pasos siguientes elevan a los usuarios de inquilinos asociados a roles de privilegios más altos con ámbito de tiempo mediante PIM:

1. Cree un grupo asignable a roles como se describe en el artículo Creación de un grupo para asignar roles en Microsoft Entra ID.

2. Vaya a Microsoft Entra ID: todos los Grupos y agregue el nuevo grupo como miembro de un grupo de seguridad para roles con privilegios elevados (por ejemplo, Administración grupo de seguridad Agentes para DAP o un grupo de seguridad correspondiente similar para roles GDAP).

3. Configure el acceso con privilegios al nuevo grupo como se describe en el artículo Asignación de propietarios y miembros aptos para grupos de acceso con privilegios.

Para más información sobre PIM, consulte ¿Qué es Privileged Identity Management?

Configuración del acceso condicional Microsoft Entra basado en riesgos

Los CSP pueden usar el acceso condicional basado en riesgos para asegurarse de que sus miembros del personal demuestren su identidad mediante MFA y cambiando su contraseña cuando se detecta como un usuario de riesgo (con credenciales filtradas o por Microsoft Entra inteligencia sobre amenazas). Los usuarios también deben iniciar sesión desde una ubicación conocida o desde un dispositivo registrado cuando se detecta como un inicio de sesión de riesgo. Otros comportamientos de riesgo incluyen el inicio de sesión desde una dirección IP malintencionada o anónima o desde una ubicación de viaje atípica o imposible, el uso de un token anómalo, el uso de una contraseña de difusión de contraseñas o la exhibición de otro comportamiento de inicio de sesión inusual. En función del nivel de riesgo de un usuario, los CSP también pueden optar por bloquear el acceso al iniciar sesión. Para obtener más información sobre los riesgos, consulte ¿Qué es el riesgo?

> ⓘ **Nota**
>
> El acceso condicional requiere una licencia Microsoft Entra ID P2 en el inquilino del asociado. Para configurar el acceso condicional, consulte **Configuración de Microsoft Entra acceso condicional**.

Contenido relacionado

Permisos de restablecimiento de contraseña (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Ver los roles de Microsoft Entra en Microsoft 365 Lighthouse (artículo)
Requisitos para Microsoft 365 Lighthouse (artículo)
Información general de Microsoft 365 Lighthouse (artículo)

Registrarse para obtener Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Revisión de los registros de auditoría en Microsoft 365 Lighthouse

Artículo • 20/01/2025

Microsoft 365 Lighthouse registros de auditoría registran acciones que generan un cambio en Lighthouse u otros servicios de Microsoft 365. Crear, editar, eliminar, asignar y acciones remotas crean eventos de auditoría que puede revisar. La auditoría está habilitada de forma predeterminada para todos los clientes. No se puede deshabilitar.

Antes de empezar

Para ver los registros de auditoría, debe tener uno de los siguientes roles:

- Administrador en Lighthouse
- agente de Administración en el Centro de partners

Revisión de los registros de auditoría

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Registros de auditoría**.

   > **Nota**
   >
   > Puede tardar hasta una hora en ver nuevos registros. Vaya al servicio correspondiente para ver los cambios más recientes.

2. Seleccione una de las pestañas siguientes para ver registros específicos: **registros de auditoría**, **registros de grafos**, **registros de directorio**, **registros de inicio de sesión**.

3. Filtre los registros, según sea necesario, mediante las siguientes opciones:

   - Pestaña Registros de auditoría
     - **Inquilinos: etiquetas** de inquilino o nombres de inquilino de cliente.
     - **Intervalo de tiempo** : último día, últimos 7 días, últimos 30 días.
     - **Actividad** : tipo de actividad de Microsoft 365 que corresponde a la acción realizada. Para obtener más información, vea la tabla Actividades .
     - **Iniciado por** : quién inició la acción.

- Pestaña Registros de grafos
  - **Inquilinos: etiquetas** de inquilino o nombres de inquilino de cliente.
  - **Intervalo de tiempo** : último día, últimos 7 días, últimos 30 días.
  - **Tipo de solicitud** : tipo de solicitud que el servicio Microsoft Graph recibió y procesó para un inquilino.
  - **Código de respuesta** : código de estado de respuesta HTTP para el evento.

- Pestaña Registros de directorio
  - **Inquilinos: etiquetas** de inquilino o nombres de inquilino de cliente.
  - **Intervalo de tiempo** : último día, últimos 7 días, últimos 30 días.
  - **Tipo** : Administración de usuarios, Administración de grupos, Administración de dispositivos, Administración de aplicaciones, Administración de roles, Administración de directivas
  - **Tipo de operación** : Agregar, Asignar, Actualizar, Quitar asignación, Eliminar API de servicio

- Pestaña Registros de inicio de sesión
  - **Inquilinos: etiquetas** de inquilino o nombres de inquilino de cliente.
  - **Intervalo de tiempo** : último día, últimos 7 días, últimos 30 días.
  - **Es interactivo** : sí (por un usuario), no (por una aplicación cliente o componentes del sistema operativo en nombre de un usuario)
  - **Estado de riesgo** : Ninguno, Seguro confirmado, Corregido, Confirmado en peligro, Descartado, En riesgo
  - **Nivel de riesgo durante el inicio de sesión** : nivel de riesgo de la sesión de inicio de sesión (probabilidad de que el inicio de sesión esté en peligro)

4. Seleccione un registro de la lista para ver los detalles completos, incluido el **cuerpo de la solicitud**.

   Para exportar datos de registro a un archivo de valores separados por comas (.csv), seleccione **Exportar**.

Actividades

En la tabla siguiente se enumeran las actividades capturadas en los registros de auditoría de Lighthouse. La lista está sujeta a cambios a medida que se crean nuevas acciones. Puede usar la actividad que aparece en el registro de auditoría para ver qué acción se inició.

Expandir tabla

Nombre de la actividad	Área en Lighthouse	Acción iniciada	Servicio afectado
aplicar o **implementar**	Espacios empresariales	Aplicación de un plan de implementación	Microsoft Entra ID, Microsoft Intune
assignTag	Espacios empresariales	Aplicación de una etiqueta desde un cliente	Faro
changeDeploymentStatus o **assign**	Espacios empresariales	Actualización del estado del plan de acción para el plan de implementación	Faro
offboardTenant	Espacios empresariales	Inactivar un cliente	Faro
resetTenantOnboardingStatus	Espacios empresariales	Reactivar un cliente	Faro
tenantTags	Espacios empresariales	Creación o eliminación de una etiqueta	Faro
tenantCustomizedInformation	Espacios empresariales	Creación, actualización o eliminación de un sitio web de cliente o información de contacto	Faro
unassignTag	Espacios empresariales	Quitar una etiqueta de un cliente	Faro
validar	Espacios empresariales	Prueba de un plan de implementación	Microsoft Entra ID
blockUserSignin	Usuarios	Bloquear inicio de sesión	Microsoft Entra ID
confirmUsersCompromised	Usuarios	Confirmación de que un usuario está en peligro	Microsoft Entra ID
dismissUsersRisk	Usuarios	Descartar el riesgo del usuario	Microsoft Entra ID

Nombre de la actividad	Área en Lighthouse	Acción iniciada	Servicio afectado
resetUserPassword	Usuarios	Restablecer contraseña	Microsoft Entra ID
setCustomerSecurityDefaultsEnabledStatus	Usuarios	Habilitación de la autenticación multifactor (MFA) con valores predeterminados de seguridad	Microsoft Entra ID
restartDevice	Dispositivos	Restart	Microsoft Intune
syncDevice	Dispositivos	Sincronizar	Microsoft Intune
rebootNow	Administración de amenazas	Reiniciar	Microsoft Intune
reprovision	Windows 365	Reintentar el aprovisionamiento	Windows 365
windowsDefenderScanFull	Administración de amenazas	Examen completo	Microsoft Intune
windowsDefenderScan	Administración de amenazas	Examen rápido	Microsoft Intune
windowsDefenderUpdateSignatures	Administración de amenazas	Actualización del antivirus	Microsoft Intune

Pasos siguientes

Use microsoft Graph API para acceder a más eventos de auditoría, si es necesario. Para obtener más información, consulte Uso de Microsoft Graph API y Administración de varios inquilinos de clientes mediante la API de Microsoft 365 Lighthouse.

Contenido relacionado

Información general de la página Alertas (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)
Ver los roles de Microsoft Entra en Microsoft 365 Lighthouse (artículo)

Comentarios

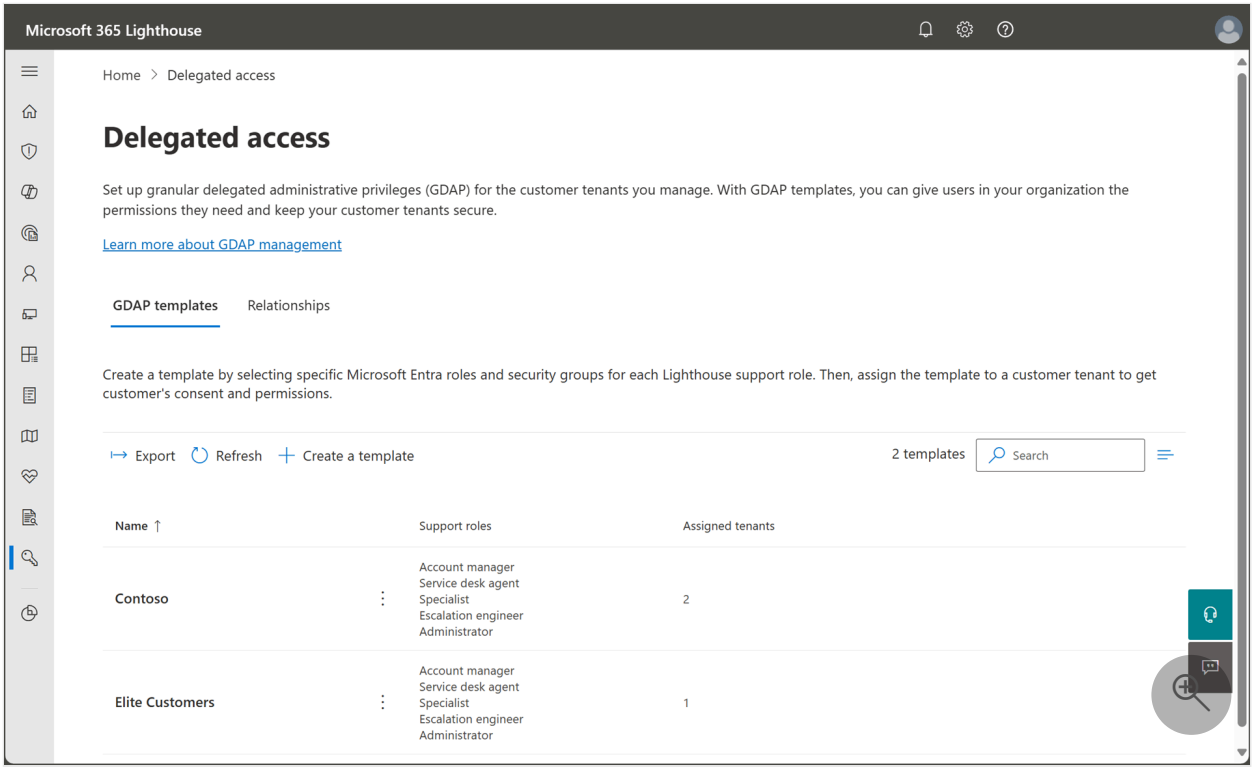
¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Información general de la página Acceso delegado en Microsoft 365 Lighthouse

Artículo • 01/10/2024

Microsoft 365 Lighthouse proporciona información de relaciones delegadas en todos los inquilinos del cliente en una sola vista. Puede crear y administrar relaciones de privilegios administrativos delegados granulares (GDAP) desde la página Acceso delegado. Los datos están disponibles para cualquier inquilino de cliente en Lighthouse, independientemente de las licencias, el número de usuarios o la región geográfica de los clientes. Para acceder a estas conclusiones, seleccione **Permisos**>**de acceso delegado** en el panel de navegación izquierdo de Lighthouse.



Requisitos de rol

En la tabla siguiente se describe el rol o los roles que debe tener para administrar las relaciones GDAP desde la página Acceso delegado.

Expandir tabla

	agente de Administración en el Centro de partners	Administrador de Grupos en Microsoft Entra ID	Administrador de usuarios en Microsoft Entra ID	Administrador de roles con privilegios en Microsoft Entra ID
Visualización de datos en la página Acceso delegado	✓			
Creación y edición de plantillas de Lighthouse GDAP		✓	✓	
Asignación de plantillas de GDAP de Lighthouse a inquilinos de clientes	✓			
Configuración del acceso Just-In-Time (JIT)				✓

Pestaña Plantillas de GDAP

En la pestaña Plantillas de GDAP, puede ver, crear, eliminar y asignar plantillas GDAP a los inquilinos del cliente. La pestaña Plantillas de GDAP proporciona la siguiente información:

- **Nombre:** Nombre de la plantilla GDAP.
- **Roles de soporte técnico:** Nombre de los roles de soporte técnico de Lighthouse asociados a cada plantilla.
- **Inquilinos asignados:** Número de inquilinos de cliente a los que está asignada la plantilla GDAP.

Seleccione una plantilla GDAP de la lista para abrir el panel de edición, donde puede actualizar el nombre, la descripción, los roles de soporte técnico y los grupos de seguridad de la plantilla.

Para asignar inquilinos a una plantilla GDAP o eliminar una plantilla GDAP, seleccione los tres puntos (más acciones) junto al nombre de la plantilla.

La pestaña Plantillas de GDAP también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar los datos de plantilla de GDAP a un archivo de valores separados por comas (.csv) de Excel.
- **Actualizar:** Seleccione esta opción para recuperar los datos de plantilla de GDAP más actuales.
- **Buscar:** Escriba palabras clave para localizar rápidamente una plantilla de GDAP específica en la lista.

Pestaña Relaciones

En la pestaña Relaciones, puede ver todas las relaciones GDAP que configuró con los clientes. La pestaña Relaciones proporciona la siguiente información:

- **Inquilino y relación:** Nombre del inquilino del cliente y relación GDAP asociada.
- **Estado:**
  - Un estado **Activo** significa que tiene al menos una relación GDAP activa con el cliente.
  - Un estado **Pendiente** indica que se ha configurado una relación GDAP, pero el cliente aún no la ha aprobado.
- **Plantilla:** Nombre de la plantilla GDAP asignada al inquilino del cliente.
- **Grupos de seguridad:** Número de grupos de seguridad asociados al inquilino del cliente.
- **Fecha de inicio:** Fecha de la relación GDAP más antigua con el cliente.
- **Fecha de caducidad:** Fecha de la relación GDAP que expirará próximamente.
- **Etiquetas:** Etiquetas asociadas al inquilino del cliente.

En la lista de inquilinos de cliente, expanda cada inquilino para mostrar las solicitudes de relación GDAP activas y pendientes. Después de que un cliente apruebe una solicitud de relación GDAP, puede seleccionar la solicitud de relación de la lista para abrir el panel de detalles de la relación y ver la siguiente información:

- Todos los grupos de seguridad y los roles de Microsoft Entra GDAP asociados al inquilino.
- Resumen de todos los roles de Microsoft Entra GDAP asociados al inquilino.

La pestaña Relaciones también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar datos de relación GDAP a un archivo de valores separados por comas (.csv) de Excel.
- **Actualizar:** Seleccione esta opción para recuperar los datos de relación GDAP más actuales.
- **Buscar:** Escriba palabras clave para localizar rápidamente una etiqueta de inquilino o inquilino específica en la lista.

Contenido relacionado

Configuración de GDAP en Microsoft 365 Lighthouse (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Configuración de la seguridad del portal de Microsoft 365 Lighthouse (artículo)
Introducción a los privilegios de administrador delegados pormenorizadas (GDAP) (artículo)
Microsoft Entra roles integrados (artículo)
Más información sobre los grupos y los derechos de acceso en Microsoft Entra ID (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Configuración de GDAP en Microsoft 365 Lighthouse

Artículo • 20/12/2024

Los privilegios administrativos delegados pormenorizadas (GDAP) son un requisito previo para que los inquilinos del cliente estén totalmente incorporados a Lighthouse. Puede configurar todos los clientes con GDAP a través de Microsoft 365 Lighthouse. Al configurar GDAP para los inquilinos del cliente que administra, puede ayudar a proteger a los clientes y garantizar que los usuarios de su organización asociada tengan los permisos necesarios para realizar su trabajo.

Para ver cómo configurar GDAP en su organización asociada, complete la guía interactiva Microsoft 365 Lighthouse segura.

Si tiene algún problema durante la instalación de GDAP y necesita instrucciones, consulte Solución de problemas y mensajes de error en Microsoft 365 Lighthouse: configuración y administración de GDAP.

Antes de empezar

- Debe tener roles específicos en Microsoft Entra ID o centro de partners, como se describe en la tabla Requisitos de rol de acceso delegado.
- Los clientes que administra en Lighthouse deben configurarse en el Centro de partners con una relación de revendedor o una relación GDAP existente.

Inspección: Configuración de GDAP

https://learn-video.azurefd.net/vod/player?id=0c8acb10-8178-4dd5-b0e8-dddc74e83684&locale=es-es&embedUrl=%2Fmicrosoft-365%2Flighthouse%2Fm365-lighthouse-setup-gdap

Echa un vistazo a los demás vídeos de Microsoft 365 Lighthouse en nuestro canal de YouTube.

Configuración de GDAP

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inicio**.
2. En la tarjeta **Configurar GDAP** , seleccione **Configurar GDAP**.

3. En la página **Acceso delegado** , seleccione la pestaña **Plantillas GDAP** y, a continuación, seleccione **Crear una plantilla**.

4. En el panel **Crear una plantilla** , escriba un nombre para la plantilla y una descripción opcional.

5. En **Roles de soporte** técnico, Lighthouse incluye cinco roles de soporte técnico predeterminados: administrador de cuentas, agente de service desk, especialista, ingeniero de escalación y administrador. Para cada rol de soporte técnico que quiera usar, haga lo siguiente:

   a. Seleccione **Editar** para abrir el panel **Editar rol de soporte** técnico.

   b. Actualice el nombre y la descripción del rol de soporte técnico, según sea necesario, para alinearse con los roles de soporte técnico de su organización asociada.

   c. En **Roles de entra**, seleccione los roles de Microsoft Entra que el rol de soporte técnico requiere en función de la función de trabajo del rol. Están disponibles las opciones siguientes:

      - Use los roles de Microsoft Entra que Recomienda Microsoft.
      - Establezca el filtro en **Todos** y seleccione los roles de Microsoft Entra preferidos.

      Para más información, consulte Microsoft Entra roles integrados.

   d. Haga clic en **Guardar**.

6. Para cada rol de soporte técnico que quiera usar, seleccione el icono **Agregar o crear un grupo de seguridad** junto al rol de soporte técnico para abrir el panel **Seleccionar o crear un grupo de seguridad** . Si no desea usar un rol de soporte técnico determinado, no le asigne ningún grupo de seguridad.

   > ⓘ **Nota**
   >
   > Cada plantilla de GDAP requiere que asigne al menos un grupo de seguridad a un rol de soporte técnico.

7. Realiza una de las siguientes acciones:

   - Para usar un grupo de seguridad existente, seleccione **Usar un grupo de seguridad existente**, elija uno o varios grupos de seguridad de la lista y, a continuación, seleccione **Guardar**.

- Para crear un nuevo grupo de seguridad, seleccione **Crear un nuevo grupo de seguridad** y haga lo siguiente:

  a. Escriba un nombre y una descripción opcional para el nuevo grupo de seguridad.

  b. Si procede, seleccione **Crear una directiva de acceso Just-In-Time (JIT) para este grupo de seguridad** y, a continuación, defina la expiración de idoneidad del usuario, la duración del acceso JIT y el grupo de seguridad del aprobador JIT.

  > ⓘ **Nota**
  >
  > Para crear una directiva de acceso Just-In-Time (JIT) para un nuevo grupo de seguridad, debe tener una licencia Microsoft Entra ID P2. Si no puede activar la casilla para crear una directiva de acceso JIT, compruebe que tiene una licencia Microsoft Entra ID P2.

  c. Agregue usuarios al grupo de seguridad y, a continuación, seleccione **Guardar**.

  > ⓘ **Nota**
  >
  > A los usuarios que forman parte de un grupo de seguridad del agente JIT no se les da acceso automáticamente a los roles de GDAP en Microsoft Entra ID. Estos usuarios primero deben solicitar acceso desde el **portal Mi acceso** y un miembro del grupo de seguridad del aprobador JIT debe revisar la solicitud de acceso JIT.

  d. Si ha creado una directiva de acceso JIT para el grupo de seguridad, puede revisar la directiva creada en el panel de gobernanza de identidades de la Centro de administración Microsoft Entra.

  Para obtener más información sobre cómo los agentes JIT pueden solicitar acceso, consulte Solicitud de acceso a un paquete de acceso en la administración de derechos.

  Para obtener más información sobre cómo los aprobadores pueden aprobar solicitudes, vea Aprobar o denegar solicitudes para roles de Microsoft Entra en Privileged Identity Management.

8. Cuando haya terminado de definir los roles de soporte técnico y los grupos de seguridad, seleccione **Guardar** en el panel **Crear una plantilla** para guardar la plantilla GDAP.

   La nueva plantilla aparece ahora en la lista de plantillas de la pestaña **Plantillas GDAP** de la página **Acceso delegado** .

9. Siga los pasos del 3 al 8 para crear más plantillas GDAP, según sea necesario.

10. En la pestaña **Plantillas de GDAP** de la página **Acceso delegado** , seleccione los tres puntos (más acciones) junto a una plantilla de la lista y, a continuación, seleccione **Asignar plantilla**.

11. En el panel **Asignar esta plantilla a inquilinos** , elija uno o varios inquilinos de cliente a los que desea asignar la plantilla y, a continuación, seleccione **Siguiente**.

    > ⓘ **Nota**
    >
    > Cada inquilino de cliente solo se puede asociar a una plantilla GDAP a la vez. Si desea asignar una nueva plantilla a un cliente, se guardan las relaciones GDAP existentes y solo se crean nuevas relaciones basadas en la nueva plantilla.

12. Revise los detalles de la asignación y, a continuación, seleccione **Asignar**.

    Las asignaciones de plantilla de GDAP pueden tardar uno o dos minutos en aplicarse. Para actualizar los datos en la pestaña **Plantillas de GDAP** , seleccione **Actualizar**.

13. Siga los pasos del 10 al 12 para asignar plantillas adicionales a los inquilinos, según sea necesario.

Obtención de la aprobación del cliente para administrar sus productos

Como parte del proceso de configuración de GDAP, se genera un vínculo de solicitud de relación GDAP para cada cliente que no tiene una relación GDAP existente con su organización asociada. Para poder administrar los productos para ellos, debe enviar el vínculo a un administrador en el inquilino del cliente para que pueda seleccionar el vínculo para aprobar la relación GDAP.

1. En la página **Acceso delegado** , seleccione la pestaña **Relaciones** .

2. Expanda el inquilino del cliente cuya aprobación necesite.

3. Seleccione la relación GDAP que muestra un estado **Pendiente** para abrir el panel de detalles de la relación.

4. Seleccione **Abrir en correo electrónico** o **Copiar correo electrónico en el Portapapeles**, edite el texto si es necesario (pero no edite la dirección URL del vínculo que necesitan seleccionar para concederle permiso de administración) y, a continuación, envíe el correo electrónico de solicitud de relación GDAP a un administrador del inquilino del cliente.

Una vez que el administrador del inquilino del cliente selecciona el vínculo para aprobar la relación GDAP, se aplica la configuración de la plantilla de GDAP. Los cambios pueden tardar hasta una hora después de la aprobación de la relación en Aparecer en Lighthouse.

Las relaciones de GDAP son visibles en el Centro de partners y los grupos de seguridad son visibles en Microsoft Entra ID.

Edición de la configuración de GDAP

Una vez completada la configuración de GDAP, puede actualizar o cambiar roles, grupos de seguridad o plantillas en cualquier momento.

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Permisos**>**de acceso delegado**.

2. En la pestaña **Plantillas de GDAP** , realice los cambios necesarios en las plantillas de GDAP o en sus configuraciones asociadas y, a continuación, guarde los cambios.

3. Asigne las plantillas GDAP actualizadas a los inquilinos de cliente adecuados para que esos inquilinos tengan las configuraciones actualizadas de las plantillas.

Contenido relacionado

Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Información general de la página Acceso delegado en Microsoft 365 Lighthouse (artículo)
Solución de problemas y mensajes de error en Microsoft 365 Lighthouse (artículo)
Configuración de la seguridad del portal de Microsoft 365 Lighthouse (artículo)
Introducción a los privilegios de administrador delegados pormenorizadas (GDAP):

Centro de partners (artículo)
Microsoft Entra roles integrados (artículo)
Más información sobre los grupos y los derechos de acceso en Microsoft Entra ID (artículo)
¿Qué es Microsoft Entra administración de derechos? (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar

Artículo • 04/06/2024

Las líneas base de Faro de Microsoft 365 proporcionan una manera repetible y escalable de administrar la configuración de seguridad de Microsoft 365 en varios inquilinos de clientes. Las líneas base proporcionan configuraciones de inquilino estándar que implementan directivas de seguridad básicas y estándares de cumplimiento que mantienen a los usuarios, dispositivos y datos de los inquilinos seguros y en buen estado.

Para ver la línea base predeterminada de Microsoft 365 Lighthouse que se aplica a todos los inquilinos, seleccione**Líneas base** de **implementación**> en el panel de navegación izquierdo de Lighthouse.

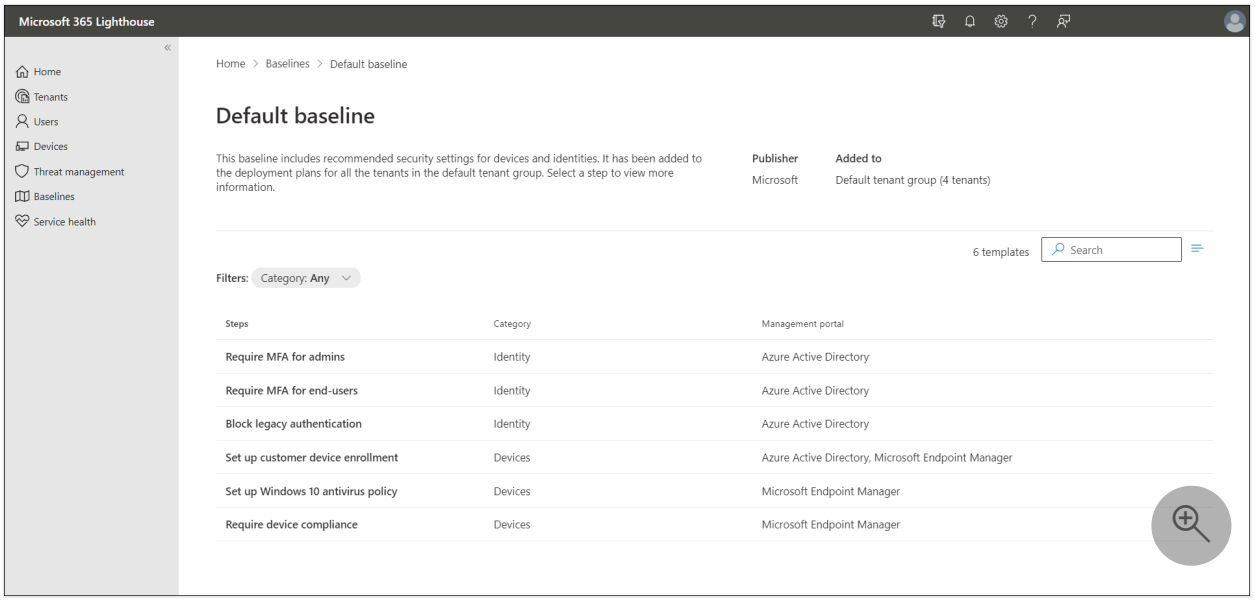
Inspección: Implementación de líneas base

https://www.microsoft.com/es-es/videoplayer/embed/RE5dQib?postJsllMsg=true&autoCaptions=es-es

Echa un vistazo a los otros vídeos de Microsoft 365 Lighthouse en nuestro canal de YouTube.

Línea base predeterminada de Microsoft 365 Lighthouse

La línea base predeterminada de Microsoft 365 Lighthouse está diseñada para garantizar que todos los inquilinos administrados estén en buen estado y sean seguros. Para ver las tareas de implementación incluidas en la línea base predeterminada, seleccione **Línea base predeterminada** en la lista. Seleccione cualquiera de las tareas de implementación para ver detalles adicionales sobre la tarea y el impacto del usuario asociado.



Categorías de línea base predeterminadas y descripciones de tareas de implementación

Expandir tabla

Categoría de línea base predeterminada	Descripción de las tareas de implementación en la categoría
Protección de identidad	Las tareas de esta categoría estandarizan las configuraciones para ayudar a proteger la identidad de un cliente y aplicar los procedimientos recomendados para ayudar a administrar las identidades de los clientes.
Protección de aplicaciones y correo electrónico	Las tareas de esta categoría estandarizan la configuración de los estándares de correo electrónico y las aplicaciones de productividad para ayudar a proteger las aplicaciones. Las tareas también aplican recomendaciones de procedimientos recomendados para asegurarse de que los clientes están protegidos contra contenido malintencionado dentro de las aplicaciones.
Inscripción de puntos de conexión	Las tareas de esta categoría garantizan que todos los dispositivos aptos del inquilino de un cliente se inscriben correctamente, se administran correctamente y usan una instalación estandarizada de aplicaciones de Microsoft 365.
Endpoint Protection	Las tareas de esta categoría se basan en las tareas de la categoría Inscripción de puntos de conexión mediante la configuración de los estándares de seguridad adecuados y la aplicación de los procedimientos recomendados para la administración diaria de dispositivos.
Protección de datos	Las tareas de esta categoría aplican recomendaciones de procedimientos recomendados para proteger a un inquilino del cliente frente a la pérdida

Categoría de línea base predeterminada	Descripción de las tareas de implementación en la categoría
	de datos y la pérdida accidental de datos confidenciales en las aplicaciones de productividad.
Experiencia del usuario final	Las tareas de esta categoría ayudan a configurar el entrenamiento para ayudar con la educación y la incorporación del usuario final. Las tareas también estandarizan la personalización de marca entre los inquilinos de los clientes para una experiencia más fluida.

Contenido relacionado

Revisión de un plan de implementación (artículo)
Introducción a las tareas de implementación (artículo)
Directivas de acceso condicional comunes (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Configuración de la seguridad del portal de Faro de Microsoft 365 (artículo)
Preguntas más frecuentes sobre Lighthouse de Microsoft 365 (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Introducción a las tareas de implementación en Microsoft 365 Lighthouse

Artículo • 04/06/2024

El plan de implementación de un inquilino se completa cuando todas las tareas son compatibles o se descartan explícitamente. Microsoft 365 Lighthouse evalúa cada tarea en función de los siguientes factores:

Expandir tabla

Factor	Description
¿El inquilino tiene licencia para los servicios necesarios asociados a la tarea?	• Las tareas que no tienen licencia no serán aptas para la implementación. • Las tareas que no tienen licencia pueden **descartarse**. • Una vez que Lighthouse detecta que el inquilino tiene licencia para los servicios necesarios asociados a la tarea, el estado se actualizará automáticamente.
¿La tarea está relacionada con otras tareas?	• Las tareas relacionadas con otras tareas deben completarse en orden secuencial. • Las tareas posteriores serán aptas para la implementación una vez que las tareas necesarias sean **compatibles**.
¿Se puede implementar la configuración asociada a la tarea a través de Lighthouse?	• Las tareas que requieren configuraciones que no se pueden implementar a través de Lighthouse requerirán una implementación manual. • Lighthouse no puede implementar tareas cuando no puede detectar ninguna configuración existente.
¿Se descartó la tarea?	• Las tareas descartadas no son aptas para la implementación. • Las tareas descartadas se pueden **reinstaurar**. • Una vez **reinstalada** una tarea, el estado se actualizará automáticamente.
¿La tarea es compatible?	• Las tareas compatibles no requieren ninguna acción adicional, pero los usuarios pueden revisar los detalles de las tareas y las configuraciones existentes.

Contenido relacionado

Implementación automática de una tarea (artículo)
Implementación manual de una tarea (artículo)
Ver detalles de la tarea (artículo)
Descartar una tarea (artículo)
Reinstalar una tarea (artículo)
Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Configuración de la seguridad del portal de Faro de Microsoft 365 (artículo)
Preguntas más frecuentes sobre Lighthouse de Microsoft 365 (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Revisión de un plan de implementación en Microsoft 365 Lighthouse

Artículo • 13/08/2023

A todos los inquilinos con un estado de incorporación **activo** se les asigna la línea base predeterminada como plan de implementación. Los planes de implementación incluyen una serie de tareas que componen el estado deseado para el inquilino. Las tareas pueden automatizarse a través de Microsoft 365 Lighthouse o requieren confirmación manual de la implementación. Las tareas relacionadas también se pueden agrupar.

Antes de empezar

Asegúrese de que usted y los inquilinos de sus clientes cumplen los requisitos enumerados en Requisitos para Microsoft 365 Lighthouse.

Además, cada usuario de inquilino de asociado debe cumplir los siguientes requisitos:

- El usuario del inquilino asociado debe tener acceso DAP/GDAP al inquilino aplicable.
    - Para DAP, el usuario del inquilino asociado debe ser miembro del grupo de agentes de administración.
    - Para GDAP, el usuario del inquilino asociado debe ser miembro de un grupo de seguridad al que se le hayan concedido permisos GDAP para la carga de trabajo aplicable asociada a la tarea.
- El usuario del inquilino del asociado debe habilitar MFA para su cuenta de usuario en el inquilino del asociado.

Acceso a un plan de implementación de inquilinos

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. En la lista de inquilinos, seleccione el inquilino que desea ver.
3. Seleccione la pestaña **Plan de implementación** .

La pestaña **Plan de implementación** enumera todas las tareas incluidas en el plan de implementación del inquilino y proporciona la siguiente información para cada tarea:

Columna	Descripción
Tarea	Nombre de la tarea.
Estado	Estado de la tarea.
Usuarios totales	Si procede, el número total de usuarios detectados dentro del inquilino.
Excluidos	Número de usuarios que se han excluido de la tarea.
No compatible	Número de usuarios cuya configuración no es compatible con la tarea.
Sin licencia	Número de usuarios a los que no se han asignado licencias a los servicios requeridos por la tarea.
No dirigido	Número de usuarios que no están destinados a la asignación de la tarea.
Compliant	Número de usuarios cuya configuración es compatible con la tarea.

La pestaña **Plan de implementación** también admite las siguientes acciones:

- **Actualizar:** Seleccione esta opción para recuperar los datos de tarea más actuales.
- **Búsqueda:** Escriba palabras clave para localizar rápidamente una tarea específica en la lista.

Cuando el estado de incorporación de un inquilino pasa a estar **activo** o al acceder a un inquilino dentro de Lighthouse, Lighthouse consulta al inquilino las configuraciones existentes. El estado de implementación se asigna a cada tarea en función del estado de cada configuración incluida en la subtarea y, si procede, para cada usuario al que se asigna la subtarea.

Los estados de implementación se determinan automáticamente por Lighthouse cuando es posible la detección y por la entrada del usuario cuando no es posible la detección.

Contenido relacionado

Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)
Introducción a las tareas de implementación (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Descripción de la información de implementación (artículo)
Configuración de la seguridad del portal de Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)

Descripción de los estados de implementación en Microsoft 365 Lighthouse

Artículo • 28/09/2024

Cuando el estado de incorporación de un inquilino pasa a estar **activo** o al acceder a un inquilino dentro de Microsoft 365 Lighthouse, Lighthouse consulta al inquilino las configuraciones existentes. El estado de implementación se asigna a cada tarea en función del estado de cada configuración incluida en la subtarea y, si procede, para cada usuario al que se asigna la subtarea.

Lighthouse determina automáticamente los estados de implementación cuando es posible la detección. Cuando no es posible la detección, Lighthouse se basa en el estado que se establece manualmente.

Las tareas pueden tener los siguientes estados:

Expandir tabla

Estado de la tarea	Descripción
Compliant	• Todos los valores incluidos en la subtarea son **compatibles**. • No hay ninguna configuración que **no sea compatible**. • No hay ninguna configuración que **falte** de todas las configuraciones existentes. Una tarea puede ser **Compatible** si una configuración es **Compatible** en una o varias configuraciones existentes sin ser **no compatible** en otra. • Puede haber **configuraciones adicionales** detectadas dentro de las configuraciones existentes.
No compatible	• Una o varias configuraciones incluidas en la subtarea **no son compatibles**. • **Falta** una o varias configuraciones de todas las configuraciones existentes. • Puede haber **configuraciones adicionales** detectadas dentro de las configuraciones existentes. **Nota:** No se aplica a las subtareas que **no tienen licencia**.
Sin licencia	El inquilino no tiene licencia para los servicios necesarios para implementar la configuración asociada a la subtarea.
Descartada	Un usuario de Lighthouse ha descartado la subtarea. **Nota:** Un usuario de Lighthouse puede descartar subtareas **sin licencia** .

Lighthouse dejará de detectar o notificar el estado de implementación de las subtareas que se han descartado.

Para determinar el estado de cada subtarea, Lighthouse detecta el estado de cada configuración incluida en la subtarea.

A la configuración se le pueden asignar los siguientes estados:

Expandir tabla

Establecer estado	Descripción
Compliant	El valor detectado en la configuración existente implementada en el inquilino del cliente es equivalente al valor del plan de implementación para todos los usuarios de destino.
No compatible	El valor detectado en la configuración existente implementada en el inquilino del cliente no es equivalente al valor del plan de implementación para uno o varios usuarios de destino.
Desaparecido	No se detecta ningún valor en el inquilino para una configuración que se incluye en el plan de implementación.
Extra	Hay un valor detectado en el inquilino para una configuración que no se incluye en el plan de implementación.

Si procede, Lighthouse detecta el estado de cada usuario para la subtarea correspondiente.

A los usuarios se les pueden asignar los siguientes estados:

Expandir tabla

Estado de usuario	Descripción
Compliant	• El usuario está destinado a la subtarea. • Al usuario se le han asignado licencias para todos los servicios requeridos por la subtarea. • Todos los valores incluidos en la subtarea son **compatibles**. • No hay ninguna configuración que **no sea compatible**. • No hay ninguna configuración que **falte** de todas las configuraciones existentes. Un usuario puede ser **Compatible** si una configuración es **Compatible** en una o varias configuraciones existentes sin ser **no compatible** en otra.

Estado de usuario	Descripción
	• Puede haber **configuraciones adicionales** detectadas dentro de las configuraciones existentes.
No compatible	• El usuario está destinado a la subtarea. • Al usuario se le han asignado licencias para todos los servicios requeridos por la subtarea. • Una o varias configuraciones incluidas en la subtarea **no son compatibles**. • **Falta** una o varias configuraciones de todas las configuraciones existentes. • Puede haber **configuraciones adicionales** detectadas dentro de las configuraciones existentes. **Nota:** No se aplica a las subtareas que **no tienen licencia**.
Excluidos	El usuario se ha excluido de la subtarea. **Nota:** Cuando un usuario se **excluye** de una subtarea, la detección de estado y los informes se actualizarán en consecuencia, pero las configuraciones existentes no se verán afectadas.
Sin licencia	El usuario no tiene licencia para los servicios necesarios para implementar la configuración prescrita. **Nota:** No se aplica a los usuarios con estado **No dirigido** .
No dirigido	El usuario no es el destino previsto para la subtarea. Por ejemplo, un usuario que no es un administrador se notifica como **No dirigido** a una subtarea que se asigna solo a los administradores.

Contenido relacionado

Introducción a las tareas de implementación en Microsoft 365 Lighthouse (artículo)
Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Configuración de la seguridad del portal de Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Descripción de la información de implementación en Microsoft 365 Lighthouse

Artículo • 28/09/2024

Microsoft 365 Lighthouse proporciona información de implementación dentro y entre los inquilinos que administra. La información de implementación se deriva de una combinación de señales detectadas por Lighthouse o introducidas en Lighthouse por un usuario en el inquilino del asociado. La información de implementación le ayuda a:

- Comprenda el estado de implementación en todos los inquilinos, usuarios y tareas del cliente.
- Revise las excepciones de implementación, como las tareas **descartadas** y los usuarios **excluidos** .
- Revise las regresiones, como las tareas que cambian de un estado **Compatible** o **Descartado** a un estado **No compatible** o **No con licencia**.
- Cuantificar las amenazas en función del progreso de la implementación en el nivel de usuario y tarea.
- Priorice las actividades de implementación en función del riesgo.

Para acceder a información de implementación, en el panel de navegación izquierdo de Lighthouse, seleccione**Deployment Deployment Insights (Información de implementación de implementación**>).

Inspección: Información de implementación

https://www.microsoft.com/es-es/videoplayer/embed/RW15vPs?postJsllMsg=true&autoCaptions=es-es

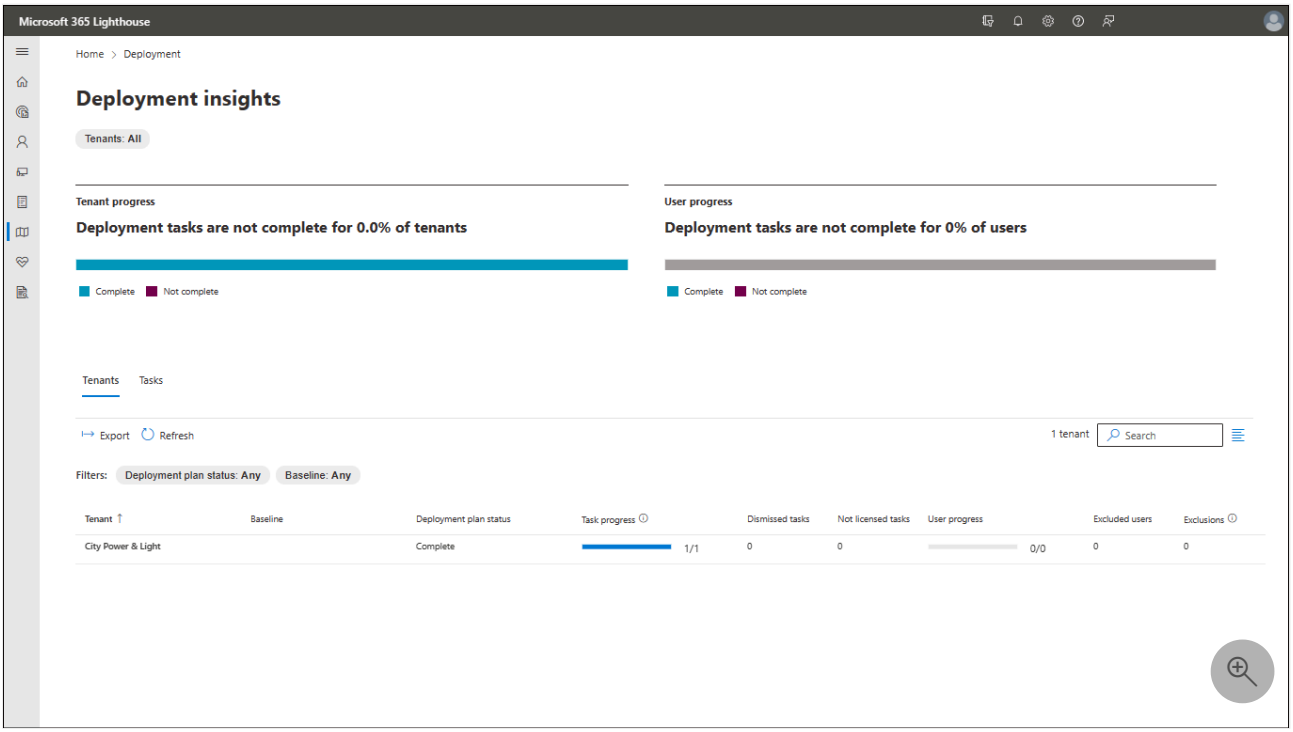
Echa un vistazo a los demás vídeos de Microsoft 365 Lighthouse en nuestro canal de YouTube.

Página información de implementación

La página **Información de implementación** incluye lo siguiente:

- Progreso del inquilino
- Progreso del usuario
- Información de implementación basada en inquilinos y tareas del cliente

> **Nota**
>
> La página **Información de implementación** mide el progreso de la implementación en todos los inquilinos de clientes que tienen un estado de incorporación **activo**. De forma predeterminada, la información de implementación se filtra para mostrar información de todos los inquilinos, pero se puede filtrar por etiqueta de inquilino.



Progreso del inquilino

El gráfico de progreso del inquilino mide el progreso de la implementación por parte del inquilino del cliente y notifica el estado del plan de implementación de cada inquilino como uno de los siguientes:

- **Completar** : el estado de todas las tareas de implementación es **Compatible** o **Descartado**.
- **No completo** : el estado de una o varias de las tareas de implementación es **No compatible** o **No tiene licencia**.

Progreso del usuario

El gráfico de progreso del usuario mide el progreso de la implementación por usuario y notifica el estado del progreso de la implementación como uno de los siguientes:

- **Completar** : el estado de todas las tareas de implementación es **Compatible**, **Excluido** o **No dirigido**.
- **No completo** : el estado de una o varias de las tareas de implementación es **No compatible** o **No tiene licencia**.

Tabla de información de implementación

La tabla de información de implementación organiza la información por inquilino y tarea del cliente.

Los datos de la pestaña **Inquilinos** se pueden filtrar por el estado del plan de implementación y la línea base. Proporciona la siguiente información para cada inquilino de cliente:

Expandir tabla

Columna	Descripción
Tenant	Nombre del inquilino del cliente.
Línea base	Línea base asignada al inquilino del cliente.

Columna	Descripción
Estado del plan de implementación	Estado del plan de implementación: **Completo** o **No completado**.
Progreso de la tarea	El número total de tareas que están en estado de finalización, ya sea **Compatible** o **Descartado**.
Tareas descartadas	Número de tareas que se han **descartado**.
Tareas sin licencia	Número de tareas para las que el inquilino del cliente **no tiene licencia**.
Tareas con regresión	El número de tareas que han retrocedido desde un estado de finalización (**compatible** o **descartado**) a un estado de **No compatible** o **Sin licencia**.
Progreso del usuario	Número de usuarios para los que todas las tareas de implementación son **Compatibles**, **Excluidas** o **No dirigidas**.
Usuarios excluidos	Número de usuarios que tienen un estado **Excluido** para una o varias tareas de implementación.
Exclusiones	Número de instancias de un usuario que tienen un estado **excluido** en todas las tareas de implementación.

Para comprender mejor la información de implementación, estos son algunos ejemplos de cómo se reflejan las distintas configuraciones de inquilino y las actividades de implementación en la tabla de información de implementación.

En este ejemplo, todos los inquilinos de clientes tienen 100 usuarios y se les ha asignado una línea base que incluye 10 tareas:

- A: completado, sin tareas que se hayan **descartado** y sin usuarios **excluidos**
- B: completado, con una tarea que se ha **descartado**
- C: completado, con 1 usuario **excluido** de 1 tarea
- D: completado, con 1 usuario **excluido** de 5 tareas
- E: completado, con 5 usuarios **excluidos** de 1 tarea
- F: completado, con 50 usuarios **excluidos** de 5 tareas
- G: completado, con 100 usuarios **excluidos** de 10 tareas
- H: no completo, con 1 usuario que no es **compatible** con 1 tarea
- I: no completo, con 1 tarea para la que 100 usuarios no son **compatibles**
- J: no completo, con 1 tarea que ha retrocedido a un estado de **No con licencia**
- K: no completo, con 1 usuario recién detectado con el estado **Sin licencia** para todas las tareas
- L: no completo, con 1 usuario desde el que se han anulado todas las licencias

Expandir tabla

Tenant	Línea base	Estado del plan de implementación	Progreso de la tarea	Tareas descartadas	Tareas sin licencia	Tareas con regresión	Progreso del usuario	Usuarios excluidos	Exclusiones de usuarios
A	Línea base predeterminada	Completo	10/10	0	0	0	100/100	0	0
N	Línea base predeterminada	Completo	10/10	1	0	0	100/100	0	0
C	Línea base predeterminada	Completo	10/10	0	0	0	100/100	1	1
D	Línea base predeterminada	Completo	10/10	0	0	0	100/100	1	5

Tenant	Línea base	Estado del plan de implementación	Progreso de la tarea	Tareas descartadas	Tareas sin licencia	Tareas con regresión	Progreso del usuario	Usuarios excluidos	Exclusiones de usuarios
E	Línea base predeterminada	Completo	10/10	0	0	0	100/100	5	5
F	Línea base predeterminada	Completo	10/10	0	0	0	100/100	50	250
G	Línea base predeterminada	Completo	10/10	0	0	0	100/100	100	1,000
H	Línea base predeterminada	No completado	9/10	0	0	0	99/100	0	0
I	Línea base predeterminada	No completado	9/10	0	0	0	0/100	0	0
J	Línea base predeterminada	No completado	9/10	0	1	1	0/100	0	0
K	Línea base predeterminada	No completado	0/10	0	0	10	99/100	0	0
L	Línea base predeterminada	No completado	0/10	0	0	10	99/100	0	0

Detalles de información de implementación por inquilino

Seleccione cualquier inquilino de cliente de la lista para abrir el panel de detalles de información de implementación de ese inquilino, que proporciona la siguiente información:

- Información general
- Tareas descartadas
- Usuarios excluidos
- Licencias necesarias

> **Nota**
>
> La información de implementación para las tareas descartadas, los usuarios excluidos y las licencias necesarias también están disponibles en la página **Inquilinos** .

Pestaña da Información general

La pestaña **Información general** proporciona el estado de cada tarea de implementación asignada al inquilino del cliente e incluye la siguiente información:

Expandir tabla

Columna	Descripción
Tareas	Nombre de la tarea.
Estado de la tarea	Estado de la tarea de implementación.

Columna	Descripción
Estado del usuario	Número de usuarios que han completado la tarea, que se han excluido de la tarea o que no se han dirigido a la tarea.

Pestaña Tareas descartadas

La pestaña **Tareas descartadas** proporciona detalles sobre las tareas que se han descartado del plan de implementación y le permite restablecer las tareas. La pestaña incluye la siguiente información:

Expandir tabla

Columna	Descripción
Tarea	Nombre de la tarea.
Reason	La razón prevista para el despido de la tarea.
Justificación	La justificación prevista para el despido de la tarea.

Pestaña Usuarios excluidos

La pestaña **Usuarios excluidos** proporciona detalles sobre los usuarios que se han excluido de una tarea de implementación. Esta pestaña incluye la siguiente información:

Expandir tabla

Columna	Descripción
Tareas con usuarios excluidos	Nombre de la tarea de la que se han excluido uno o varios usuarios.
Usuarios excluidos	Los nombres de cada usuario que se ha excluido.

Pestaña Licencias necesarias

La pestaña **Licencias necesarias** proporciona detalles sobre las tareas de implementación en las que uno o más usuarios requieren licencias adicionales para completar la tarea. Esta pestaña incluye la siguiente información:

Expandir tabla

Columna	Descripción
Tareas con usuarios sin licencia	Nombre de la tarea para la que uno o varios usuarios no tienen licencia.
Usuarios sin licencia	Nombre de cada usuario que no tiene licencia para completar la tarea.

Tabla de información de implementación por tarea

Para ver la información de implementación por tarea, seleccione la pestaña **Tareas** . Los datos de la pestaña **Tareas** se pueden filtrar por línea base y proporciona la siguiente información:

Expandir tabla

Columna	Descripción
Tarea	Nombre de la tarea.
Línea base	Línea base asociada a la tarea.
Inquilinos asignados	Número de inquilinos a los que se ha asignado esta tarea.
Compliant	Número de inquilinos con un estado de tarea **compatible**.
No compatible	Número de inquilinos con un estado de tarea **no compatible**.
Descartada	Número de inquilinos con un estado de tarea **descartado**.
Sin licencia	Número de inquilinos con un estado de tarea **sin licencia**.

Seleccione cualquier tarea de la lista para abrir el panel de detalles de información de implementación de esa tarea, que proporciona la siguiente información:

Expandir tabla

Columna	Descripción
Tenant	Nombre del inquilino del cliente.
Estado de la tarea	Estado de implementación de la tarea para el inquilino.
Usuarios totales	Número de usuarios asignados a la tarea.
Usuarios compatibles	El número de usuarios que son **compatibles**.
Usuarios no conformes	Número de usuarios que no son **compatibles**.

Pasos siguientes

Para obtener información sobre cómo administrar inquilinos mediante información de implementación, consulte Administración de inquilinos mediante información de implementación en Microsoft 365 Lighthouse.

Contenido relacionado

Introducción a las tareas de implementación en Microsoft 365 Lighthouse (artículo)
Información general sobre el uso de líneas base de Micrososft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)
Descripción de los estados de implementación en Microsoft 365 Ligthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Ver los detalles de la tarea en Microsoft 365 Lighthouse

Artículo • 13/08/2023

Microsoft 365 Lighthouse proporciona información detallada sobre cada tarea dentro de un plan de implementación del cliente. Al ver el plan de implementación de un inquilino, todas las tareas para las que Lighthouse puede detectar configuraciones existentes tendrán un estado asignado para cada configuración y, si procede, cada usuario.

De forma predeterminada, cada tarea se designa como **Compatible**, **No compatible** o **Sin licencia**. Para obtener una definición de los estados de implementación, consulte Descripción de los estados de implementación en Microsoft 365 Lighthouse. Puede implementar, descartar o restablecer tareas desde esta vista.

Antes de empezar

Asegúrese de que usted y los inquilinos de sus clientes cumplen los requisitos enumerados en Requisitos para Microsoft 365 Lighthouse.

Además, cada usuario de inquilino de asociado debe cumplir los siguientes requisitos:

- El usuario del inquilino asociado debe tener acceso DAP/GDAP al inquilino aplicable.
    - Para DAP, el usuario del inquilino asociado debe ser miembro del grupo de agentes de administración.
    - Para GDAP, el usuario del inquilino asociado debe ser miembro de un grupo de seguridad al que se le hayan concedido permisos GDAP para la carga de trabajo aplicable asociada a la tarea.
- El usuario del inquilino del asociado debe habilitar MFA para su cuenta de usuario en el inquilino del asociado.

Ver detalles de la tarea

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. Seleccione un inquilino activo.
3. En la página del inquilino, seleccione la pestaña **Plan de implementación** .

4. En la lista de tareas, seleccione una tarea para ver más detalles.

El panel de detalles de la tarea proporciona información general de la tarea, información de progreso del usuario de la tarea y un historial de estado de la tarea de los 30 días anteriores.

La pestaña Información general proporciona la siguiente información:

Detalles	Descripción
Estado	Estado de implementación de la tarea.
Descripción	Descripción de la tarea.
Línea base	Línea base asignada al inquilino.
Categoría	La categoría de tarea (por ejemplo, Identidad, Dispositivos o Datos).
Servicios requeridos	Los servicios necesarios para la finalización de la tarea.
Portal de administración	Portal de administración donde se administra la configuración asociada a la tarea.
Impacto en el usuario	Impacto de la implementación de la configuración asociada con la tarea a los usuarios del inquilino.
Para los usuarios	Vínculos a recursos adicionales.

La pestaña Progreso de la implementación proporciona el estado del usuario asociado a la tarea. Los usuarios son compatibles cuando todas las configuraciones son **compatibles** o **adicionales,** y no **falta** ninguna configuración o **no es compatible**. No se notifica ningún progreso para las tareas que se han descartado.

La pestaña Historial de detección muestra una vista gráfica de cada vez que Lighthouse ha examinado el inquilino para detectar su configuración en los 30 días anteriores, lo que proporciona el estado de implementación de la tarea y el número de usuarios en cada estado de implementación para cada examen.

Contenido relacionado

Implementación manual de una tarea (artículo)
Implementación automática de una tarea (artículo)
Descartar una tarea (artículo)
Reinstalar una tarea (artículo)
Introducción a las tareas de implementación en Microsoft 365 Lighthouse (artículo)
Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para

implementar configuraciones de inquilino estándar (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Configuración de la seguridad del portal de Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)

Asignación de una línea base en Microsoft 365 Lighthouse

Artículo • 21/10/2024

De forma predeterminada, Microsoft 365 Lighthouse asigna la línea base predeterminada a todos los inquilinos. Puede crear y asignar una línea base para adaptarse a los distintos requisitos del cliente.

> **Nota**
>
> Algunas características se implantan a diferentes velocidades para nuestros clientes. Si aún no ve una característica, debería verla pronto.
>
> Para ver qué nuevas características están disponibles actualmente en el inquilino del asociado, vaya a la página **principal** de Microsoft 365 Lighthouse y, a continuación, seleccione el vínculo **Novedades** de la esquina superior derecha de la página o seleccione **Novedades** de la tarjeta **Novedades & recursos de aprendizaje** .

Antes de empezar

Asegúrese de que usted y los inquilinos de sus clientes cumplen los requisitos enumerados en Requisitos para El faro de Microsoft 365.

Además, cada usuario de inquilino de asociado debe ser administrador de Lighthouse de Microsoft 365.

Asignación de una línea base a un inquilino

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. Seleccione un inquilino al que desea asignar una nueva línea base.
3. Seleccione **Asignar línea base**.
4. Seleccione la línea base que desea asignar a los inquilinos seleccionados.

> **Nota**
>
> Las líneas base no incluyen atributos específicos del inquilino y la asignación de una nueva línea base sobrescribirá cualquier personalización preexistente en la

configuración del plan de implementación de un inquilino, como los despidos de tareas de implementación, las exclusiones de usuarios y grupos de usuarios y los estados de implementación de las tareas de implementación manual. Estos valores tendrán que volver a escribirse para cada inquilino, según sea necesario.

Pasos siguientes

Una vez asignada la línea base, Lighthouse consulta a los inquilinos asignados para detectar e informar de su estado de implementación. Revise el plan de implementación para determinar los pasos siguientes en el proceso de implementación.

Contenido relacionado

Creación de líneas base (artículo)
Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Lighthouse de Microsoft 365 (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Creación de una línea base en Microsoft 365 Lighthouse

Artículo • 20/01/2025

Microsoft 365 Lighthouse le permite crear sus propias líneas base para implementarlas en los inquilinos del cliente. Cree sus propias líneas base para dar cabida a los clientes con distintos grados de madurez del inquilino, clientes de diferentes sectores, clientes que se han suscrito a diferentes servicios administrados de su empresa o clientes con distintos modelos de licencia.

Antes de empezar

- Asegúrese de que usted y los inquilinos de sus clientes cumplen los requisitos enumerados en Requisitos para Microsoft 365 Lighthouse.
- Debe tener el rol Administrador o Autor en Lighthouse.

Creación de una línea base

Hay tres maneras de crear una línea base en Lighthouse. Puede clonar una línea base existente, importar una línea base o crear una nueva línea base.

Para clonar una línea base existente:

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Líneas basede implementación**>.
2. En la lista de líneas base, seleccione la línea base que desea clonar.
3. Seleccione **Clonar**

> **Nota**
>
> La nueva línea base será el nombre de la línea base desde la que se clonó con "(1)" agregado al final.

Para crear una nueva línea base:

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Líneas basede implementación**>.

2. Seleccione **Crear**.
3. Proporcione un nombre para mostrar y una descripción para la nueva línea base.
4. Seleccione **Crear**.

Para importar una línea base:

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Líneas basede implementación**>.
2. Seleccione **Importar**.
3. Seleccione el archivo de línea base deseado.
4. Seleccione **Importar**.

> **Nota**
>
> Las líneas base se pueden editar, eliminar y exportar desde la página. La línea base predeterminada no se puede editar ni eliminar.
>
> Todas las líneas base, excepto la línea base predeterminada, se pueden exportar desde Lighthouse como archivos JSON. Las líneas base también se pueden importar a Lighthouse seleccionando un archivo JSON que haya sido:
>
> - Extraído de Lighthouse
> - Extraído de Lighthouse y editado
> - Creado fuera de Lighthouse
>
> Para obtener más información, consulte Visualización de JSON con formato.

Adición de una tarea de implementación a una línea base

Las líneas base se componen de tareas de implementación. Puede agregar tantas tareas de implementación como desee a una línea base. Hay dos maneras de agregar tareas de implementación a una línea base. Puede clonar una tarea de implementación de una línea base existente o extraer una configuración de un inquilino administrado.

Para clonar una tarea de implementación desde una línea base existente:

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Líneas basede implementación**>.
2. Seleccione una línea base de la lista.
3. Seleccione **Nueva tarea**.
4. En la lista, seleccione **Clonar**.
5. En el panel **Nueva tarea** , seleccione la línea de base que contiene la tarea que desea clonar.
6. Seleccione la tarea de implementación que desea clonar.
7. Seleccione **Clonar**.

Para extraer una configuración de un inquilino administrado:

> **Importante**
>
> Las configuraciones extraídas pueden contener valores de configuración específicos del inquilino que se deben quitar de una línea base para evitar aplicarlas a otros inquilinos administrados.

Lighthouse, siempre que sea posible, detecta configuraciones y directivas que contienen información confidencial y quita el valor específico del inquilino de la línea base. Sin embargo, hay algunos tipos de configuración en los que los valores de configuración confidenciales deben detectarse y quitarse manualmente para asegurarse de que no se incluyen en la línea base.

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Líneas basede implementación**>.
2. Seleccione una línea base de la lista.
3. Seleccione **Nueva tarea**.
4. En la lista, seleccione la configuración deseada.
5. Seleccione el inquilino del que desea extraer la configuración.
6. Seleccione la configuración que desea extraer.
7. Seleccione **Siguiente**.
8. Proporcione el nombre para mostrar, la descripción y los detalles del impacto del usuario.
9. Revise la tarea para asegurarse de que se quitan los valores de configuración específicos del inquilino que no deben aplicarse a otros inquilinos administrados.
10. Si procede, seleccione el icono **Quitar** para quitar los valores de configuración específicos del inquilino.
11. Seleccione **Crear**.

> **Nota**

Para editar una tarea de implementación, seleccione el icono de lápiz en la columna **Acción** . Para eliminar una tarea de implementación, seleccione el icono de papelera en la columna **Acción** . Para aumentar o reducir la prioridad de una tarea, seleccione una flecha en la columna **Prioridad** .

Pasos siguientes

Una vez creada una línea base, puede asignar la línea base a un inquilino. Para obtener más información, consulte Asignación de una línea base.

Contenido relacionado

Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Implementación manual de una tarea en Microsoft 365 Lighthouse

Artículo • 04/06/2024

Las tareas que requieren configuraciones que no se pueden implementar automáticamente a través de Microsoft 365 Lighthouse requieren una implementación manual. Una vez completada la implementación manual, establezca el estado de la tarea en **Compatible** para reflejar el estado actual de la tarea.

Antes de empezar

Asegúrese de que usted y los inquilinos de sus clientes cumplen los requisitos enumerados en Requisitos para El faro de Microsoft 365.

Además, cada usuario de inquilino de asociado debe cumplir los siguientes requisitos:

- El usuario del inquilino asociado debe tener acceso DAP/GDAP al inquilino aplicable.
    - Para DAP, el usuario del inquilino asociado debe ser miembro del grupo de agentes de administración.
    - Para GDAP, el usuario del inquilino asociado debe ser miembro de un grupo de seguridad al que se le hayan concedido permisos GDAP para la carga de trabajo aplicable asociada a la tarea.
- El usuario del inquilino del asociado debe habilitar MFA para su cuenta de usuario en el inquilino del asociado.

Implementación manual de una tarea

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. En la lista de inquilinos, seleccione el inquilino que desea ver.
3. Seleccione la pestaña **Plan de implementación** .
4. En la lista de tareas, seleccione la tarea que desea implementar manualmente.
5. En el panel de detalles de la tarea, seleccione **Marcar como compatible**.

6. En el cuadro de diálogo de confirmación, escriba su nombre tal y como aparece en Lighthouse.
7. Haga clic en **Guardar**.

El estado de la tarea se actualizará a **Compatible** y el panel Detalles de la tarea reflejará qué usuario de Lighthouse completó los pasos de implementación.

Si el estado de la tarea cambia y ya no es compatible, puede restablecer el estado a **No compatible**. Para hacerlo:

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. En la lista de inquilinos, seleccione el inquilino que desea ver.
3. Seleccione la pestaña **Plan de implementación** .
4. En la lista de tareas, seleccione la tarea que desea actualizar.
5. En el panel de detalles de la tarea, seleccione **Marcar como no compatible**.
6. En el cuadro de diálogo **Marcar tarea como no compatible** , seleccione **Guardar**.

Las tareas que se deben implementar manualmente también se pueden descartar independientemente de su estado de implementación. Las tareas que se han descartado después de establecerse como **Compatibles** volverán a **No compatible** cuando se vuelvan a instalar.

Contenido relacionado

Implementación automática de una tarea (artículo)
Descartar una tarea (artículo)
Reinstalar una tarea (artículo)
Introducción a las tareas de implementación en Microsoft 365 Lighthouse (artículo)
Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Configuración de la seguridad del portal de Faro de Microsoft 365 (artículo)
Preguntas más frecuentes sobre Lighthouse de Microsoft 365 (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Implementación automática de una tarea en Microsoft 365 Lighthouse

Artículo • 11/08/2023

Microsoft 365 Lighthouse permite implementar automáticamente configuraciones asociadas a tareas de implementación aptas. Esta funcionalidad ayuda a garantizar que los inquilinos que administra estén en buen estado y sean seguros.

Antes de empezar

Asegúrese de que usted y los inquilinos de sus clientes cumplen los requisitos enumerados en Requisitos para Microsoft 365 Lighthouse.

Además, cada usuario de inquilino de asociado debe cumplir los siguientes requisitos:

- El usuario del inquilino asociado debe tener acceso DAP/GDAP al inquilino aplicable.
    - Para DAP, el usuario del inquilino asociado debe ser miembro del grupo de agentes de administración.
    - Para GDAP, el usuario del inquilino asociado debe ser miembro de un grupo de seguridad al que se le hayan concedido permisos GDAP para la carga de trabajo aplicable asociada a la tarea.
- El usuario del inquilino del asociado debe habilitar MFA para su cuenta de usuario en el inquilino del asociado.

Implementación automática de una tarea

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. En la lista de inquilinos, seleccione un inquilino que quiera ver.
3. Seleccione la pestaña **Plan de implementación** .
4. Seleccione una tarea de la lista.
5. En el panel de detalles de la tarea, seleccione **Implementar**.
6. En la página **Revisar tarea de implementación** , edite la configuración predeterminada según sea necesario.

a. Si procede, seleccione si desea implementar la configuración como **modo Habilitar** o **Solo informe** .

b. Si procede, edite la asignación de la tarea para:

i. Incluir o excluir usuarios específicos.

ii. Incluir o excluir grupos de seguridad.

> ⓘ **Nota**
>
> Las tareas implementadas por una implementación de directiva de acceso condicional incluyen un menú desplegable para seleccionar el estado de implementación. Las tareas se establecen en el estado de implementación **Habilitado** de forma predeterminada, pero se pueden ajustar manualmente a **Solo** informe a través del menú desplegable. Las tareas implementadas como **Habilitadas** afectarán inmediatamente a la experiencia del usuario. La configuración de las configuraciones implementadas en un estado **Solo** informe se seguirá notificando como **No compatible** en Lighthouse hasta que el estado de implementación de la configuración aplicable se actualice a **Habilitado**.

7. Seleccione **Siguiente**.

8. En la página **Revisar configuración de inquilino** , revise las configuraciones de intersección. Las configuraciones de intersección son propiedades comunes con valores que también se incluyen en la tarea de implementación.

   La página **Revisar configuraciones de inquilino** se proporciona para las tareas aptas y enumera las configuraciones de intersección detectadas en el inquilino. Desde esta página, puede editar las configuraciones existentes o implementar una nueva configuración a través de Lighthouse para cumplir los requisitos de la tarea.

   Si se detectan configuraciones existentes, se mostrarán con un vínculo a la configuración aplicable en la **configuración Detectada de la** tabla de comparación del plan de implementación.

   La tabla de configuraciones detectadas en la parte inferior de la página permite comparar las configuraciones detectadas del inquilino con el plan de implementación, incluidas las selecciones realizadas en la página **revisar la tarea de implementación** . Esta tabla se puede filtrar por configuración o por estado de configuración y el usuario puede buscarla.

Si no hay ninguna configuración detectada, se le dirigirá a la página **Confirmar configuración** .

9. Si procede, edite las configuraciones existentes según sea necesario.

    a. Abra el portal de administración adecuado.

    b. Vaya a la configuración adecuada.

    c. Edite la configuración según sea necesario para la tarea.

    d. Guardar la configuración actualizada en el portal de administración aplicable

    e. En Lighthouse, seleccione **Actualizar** para actualizar los resultados de la configuración detectada.

    Al editar las configuraciones existentes, la configuración **adicional** no afecta al estado de implementación de la tarea. Puede conservar, editar o descartar la configuración **adicional** a su discreción.

    Una vez que Lighthouse determina que no hay ninguna configuración que **no sea compatible** o que **falte** de todas las configuraciones existentes, Lighthouse actualizará el estado de la tarea a **Compatible**. Se le pedirá que salga del asistente.

10. Seleccione **Siguiente**.

11. En la página **Confirmar configuración** , confirme la configuración y seleccione **Confirmar**.

12. En la página **Completar** confirmación, seleccione **Cerrar**.

La implementación de una nueva configuración a través de Lighthouse garantizará que se aplique la configuración de seguridad, pero no modificará ninguna configuración existente. Esto puede dar lugar a una configuración con valores duplicados o en conflicto para los usuarios, lo que puede impedir que el estado de la tarea se actualice a **Compatible**. Para que la tarea sea compatible, deberá editar o eliminar la configuración que no sea compatible con la tarea de implementación.

Contenido relacionado

Implementación manual de una tarea (artículo)
Descartar una tarea (artículo)
Reinstalar una tarea (artículo)
Introducción a las tareas de implementación en Microsoft 365 Lighthouse (artículo)
Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para

implementar configuraciones de inquilino estándar (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Configuración de la seguridad del portal de Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)

Descartar una tarea en El faro de Microsoft 365

Artículo • 04/06/2024

Puede descartar tareas del plan de implementación en el que un proveedor de servicios administrados (MSP) decide aceptar el riesgo asociado de no completar la tarea o resolver la tarea a través de un tercero u otra mitigación alternativa. El despido de una tarea no afecta a la configuración del inquilino administrado. Una vez descartado, Microsoft 365 Lighthouse ya no detectará configuraciones ni notificará el estado de implementación de esa tarea. Las tareas se pueden descartar o restablecer en cualquier momento.

Antes de empezar

Asegúrese de que usted y los inquilinos de sus clientes cumplen los requisitos enumerados en Requisitos para El faro de Microsoft 365.

Además, cada usuario de inquilino de asociado debe cumplir los siguientes requisitos:

- El usuario del inquilino asociado debe tener acceso DAP/GDAP al inquilino aplicable.
    - Para DAP, el usuario del inquilino asociado debe ser miembro del grupo de agentes de administración.
    - Para GDAP, el usuario del inquilino asociado debe ser miembro de un grupo de seguridad al que se le hayan concedido permisos GDAP para la carga de trabajo aplicable asociada a la tarea.
- El usuario del inquilino del asociado debe habilitar MFA para su cuenta de usuario en el inquilino del asociado.

Descartar una tarea

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. Seleccione el inquilino adecuado en la lista.
3. Seleccione **la pestaña Plan de implementación** .
4. En la lista de tareas, seleccione la tarea que desea descartar.

5. En el panel de detalles de la tarea, seleccione **Descartar**.
6. Seleccione uno de los siguientes motivos para descartar la tarea:
    a. Riesgo aceptado
    b. Resuelto a través de terceros
    c. Resuelto mediante mitigación alternativa
7. En el campo Justificación, proporcione un motivo para descartar la tarea.
8. Haga clic en **Guardar**.

También puede seleccionar la opción **Más acciones** (icono de puntos suspensivos) directamente en la lista de tareas para descartar la tarea.

Pasos siguientes

Si cambia el estado de una tarea descartada, puede restablecerla. Para obtener más información, consulte Reinstalar una tarea en Microsoft 365 Lighthouse.

Contenido relacionado

Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Configuración de la seguridad del portal de Faro de Microsoft 365 (artículo)
Preguntas más frecuentes sobre Lighthouse de Microsoft 365 (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Reinstalar una tarea en El faro de Microsoft 365

Artículo • 04/06/2024

Puede restablecer una tarea de implementación descartada en Microsoft 365 Lighthouse.

Antes de empezar

Asegúrese de que usted y los inquilinos de sus clientes cumplen los requisitos enumerados en Requisitos para El faro de Microsoft 365.

Además, cada usuario de inquilino de asociado debe cumplir los siguientes requisitos:

- El usuario del inquilino asociado debe tener acceso DAP/GDAP al inquilino aplicable.
    - Para DAP, el usuario del inquilino asociado debe ser miembro del grupo de agentes de administración.
    - Para GDAP, el usuario del inquilino asociado debe ser miembro de un grupo de seguridad al que se le hayan concedido permisos GDAP para la carga de trabajo aplicable asociada a la tarea.
- El usuario del inquilino del asociado debe habilitar MFA para su cuenta de usuario en el inquilino del asociado.

Reinstalar una tarea

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. Seleccione el inquilino adecuado en la lista.
3. Seleccione **la pestaña Plan de implementación** .
4. En la lista de tareas, seleccione la tarea que desea restablecer.
5. En el panel de detalles de la tarea, seleccione **Reinstate (Restablecer)**.
6. En el cuadro de diálogo **Reinstate task (Restablecer tarea**), seleccione **Reinstate (Restablecer)**.

También puede seleccionar la opción **Más acciones** (icono de puntos suspensivos) directamente en la lista de tareas para restablecer la tarea. Una vez que se restablece una tarea, la detección de estado y los informes se actualizarán en consecuencia.

Pasos siguientes

Si desea investigar por qué se ha descartado una tarea, puede auditar la excepción mediante información de implementación. Para obtener más información, consulte Administración de inquilinos mediante información de implementación en Microsoft 365 Lighthouse.

Contenido relacionado

Descartar una tarea en Microsoft 365 Lighthouse (artículo)
Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Configuración de la seguridad del portal de Faro de Microsoft 365 (artículo)
Preguntas más frecuentes sobre Lighthouse de Microsoft 365 (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Administración de inquilinos mediante información de implementación en Microsoft 365 Lighthouse

Artículo • 03/10/2024

Microsoft 365 Lighthouse proporciona información de implementación dentro y entre los inquilinos que administra. La vista única le permite:

- Comprenda el estado de implementación en todos los inquilinos, usuarios y tareas.
- Revise las excepciones de implementación, como las tareas **descartadas** y los usuarios **excluidos** .
- Revise las regresiones, como las tareas que cambian de un estado **Compatible** o **Descartado** a un estado **No compatible** o **No con licencia**.
- Cuantificar las amenazas en función del progreso de la implementación en el nivel de usuario y tarea.
- Priorice las actividades de implementación en función del riesgo.

Administración del progreso de la implementación mediante información de implementación

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Información de implementación** de **implementación**>.

2. En la página **Información de implementación** , revise las siguientes áreas para recopilar información sobre el progreso de la implementación de los inquilinos del cliente.

Expandir tabla

Área	Descripción
Progreso del inquilino	Proporciona un resumen del progreso de la implementación en todos los inquilinos. Puede mantener el puntero sobre el gráfico para ver el número de inquilinos con planes de implementación **completados** y **no completados**. Los inquilinos para los que todas las tareas asignadas son **Compatibles** o **Descartadas se** consideran **Completadas**. Los inquilinos para los que una o varias tareas asignadas **no son compatibles** o **no tienen licencia** se consideran **No completadas**.

Área	Descripción
Progreso del usuario	Proporciona un resumen de progreso de implementación de usuario para todos los usuarios. Puede mantener el puntero sobre el gráfico para ver el número exacto de usuarios **completados yno completados**. Los usuarios para los que todas las tareas asignadas son **Compatibles**, **Descartadas** o **No dirigidas** se consideran **Completadas**. Los usuarios para los que una o varias tareas asignadas **no son compatibles** o **no tienen licencia** se consideran **No completadas**.
Pestaña Inquilinos	Proporciona un progreso de implementación detallado para cada inquilino. Puede usar varios puntos de datos de la tabla para determinar la acción adecuada. Por ejemplo, la columna **Tareas sin licencia** indica el número de tareas para las que el inquilino no tiene licencia. Para resolver el problema, puede agregar una licencia o excluir al usuario de la tarea. La columna **Tareas con regresión** indica que un estado de tarea cambió de un estado **Compatible** o **Descartado** . Puede ir al plan de implementación de inquilinos específico y realizar la acción adecuada.
Pestaña Tareas	Proporciona el progreso de la implementación para todas las tareas, incluido el número de inquilinos a los que se asigna la tarea. En el caso de las tareas que **no son compatibles** o **no tienen licencia**, puede tomar medidas para resolver el problema.

Para obtener soluciones adicionales para problemas de implementación comunes, consulte la sección Implementación de líneas base en Microsoft 365 Lighthouse preguntas más frecuentes (P+F).

Revisión de tareas regresadas

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Información de implementación** de **implementación**>.
2. En la pestaña **Inquilinos** , busque los inquilinos que tengan un número distinto de **0** en la columna **Tareas con regresión** .
3. Seleccione el inquilino deseado para abrir la página de detalles del inquilino y ver las tareas regresadas.
4. Para ver el plan de implementación del inquilino, seleccione **Ver plan de implementación de inquilinos**.
5. En la pestaña **Plan de implementación** , seleccione la tarea regresiva de la lista para abrir el panel de detalles de la tarea.
6. Revise la configuración del inquilino y, en función del escenario de regresión, modifique la tarea de implementación, modifique la configuración del inquilino, modifique las licencias del inquilino o descarte la tarea para resolver la regresión.

Auditoría de excepciones de implementación mediante información de implementación

Cada tarea descartada y un usuario excluido representan una amenaza potencial. Puede auditar estas excepciones para asegurarse de que siguen cumpliendo sus requisitos.

Auditoría de tareas descartadas

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Información de implementación** de **implementación**>.
2. En la pestaña **Inquilinos** , seleccione un inquilino que tenga un número distinto de **0** en la columna **Tareas descartadas** para abrir el panel de detalles del inquilino.
3. En el panel de detalles del inquilino, seleccione la pestaña **Tareas descartadas** .
4. En la lista de tareas descartadas, revise el motivo y la justificación de cada tarea para determinar si el despido sigue siendo válido.
5. Si ya no es válido, seleccione la tarea descartada de la lista y, a continuación, seleccione **Restablecer**.

Auditoría de usuarios excluidos

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Información de implementación** de **implementación**>.
2. En la pestaña **Inquilinos** , seleccione un inquilino que tenga un número distinto de **0** en la columna **Usuarios excluidos** para abrir el panel de detalles del inquilino.
3. En el panel de detalles del inquilino, seleccione la pestaña **Usuarios excluidos** .
4. En la lista de tareas con usuarios excluidos, expanda cada tarea y determine si el usuario enumerado debe seguir excluyendo.
5. Si ya no se debe excluir un usuario, seleccione **Ver plan de implementación de inquilinos**.
6. En la pestaña **Plan de implementación** , seleccione la tarea de implementación aplicable en la lista para abrir el panel de detalles de la tarea.
7. Seleccione **Implementar**.

8. En la página **Revisar tarea de implementación** , quite el usuario del cuadro **Excluir usuarios** y, a continuación, seleccione **Siguiente**.

9. En la página **Revisar configuraciones de inquilino** , revise las configuraciones y, a continuación, seleccione **Siguiente**.

10. En la página **Confirmar configuración** , revise los valores de configuración y, a continuación, seleccione **Implementar**.

Contenido relacionado

Introducción a las tareas de implementación (artículo)
Información general sobre el uso de líneas base para implementar configuraciones de inquilino estándar (artículo)
Descripción de los estados de implementación (artículo)
Microsoft 365 Lighthouse preguntas más frecuentes (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Información general de la página Alertas de Microsoft 365 Lighthouse

Artículo • 09/08/2024

Como proveedor de MSP, debe supervisar y responder a los problemas de seguridad de sus clientes de forma eficaz y eficaz. Microsoft 365 Lighthouse presenta alertas, una herramienta eficaz que proporciona una vista consolidada de todas las detecciones y alertas de alta prioridad entre los clientes. Puede ver una lista con prioridad de los problemas más urgentes que requieren su atención y tomar medidas inmediatas para resolverlos. También puede habilitar las alertas de inserción en los sistemas y flujos de soporte técnico existentes, de modo que nunca se pierda una alerta crítica que necesite su intervención.

Para ayudarle a empezar, Lighthouse proporciona un conjunto predeterminado de reglas de alerta basadas en procedimientos recomendados y recomendaciones. Puede usar estas reglas de alerta tal como están o modificarlas según sus preferencias y necesidades. También puede crear reglas de alerta personalizadas para obtener más control y flexibilidad.

Ficha Alertas

La pestaña **Alertas** proporciona una vista consolidada de posibles problemas de seguridad en todos los clientes. La pestaña contiene dos secciones:

- **Alertas activas por fecha de creación**: gráfico que muestra el número de alertas activas a lo largo del tiempo.
- **Tabla de alertas**: una lista de alertas actuales que se pueden filtrar por tipo de alerta, gravedad, estado o asignado.

La pestaña **Alertas** también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar los datos de alerta a un archivo de valores separados por comas (.csv) de Excel.
- **Actualizar:** Seleccione esta opción para recuperar los datos de alerta más actuales.
- **Buscar:** Escriba palabras clave para buscar una alerta específica en la lista.

En la lista de alertas, seleccione cualquier alerta para abrir el panel de detalles de la alerta. La pestaña **Información general** de este panel incluye la siguiente información:

- Inquilinos afectados

- Descripción de la alerta
- Regla que desencadenó la alerta
- Tipo de alerta
- Marca de tiempo (se detectó por primera vez y se actualizó por última vez)
- Entidad afectada

En la pestaña **Información general** , puede actualizar la gravedad y el estado de la alerta y asignar la alerta a un usuario específico para resolverla.

Seleccione la pestaña **Comentarios e historial** en el panel de detalles de la alerta para ver un historial completo de la alerta. Puede agregar comentarios adicionales a la alerta según sea necesario.

Tipo de alerta

Lighthouse ofrece varios tipos de alerta configurables de los siguientes servicios: Microsoft Defender para empresas (MDB), Antivirus de Microsoft Defender e Id. de Microsoft Entra.

Lighthouse *no* admite actualmente alertas de los siguientes servicios: Microsoft Defender for Cloud Apps, Microsoft Defender para Office 365 (MDO) o servicios adicionales de Azure.

En la tabla siguiente se proporcionan detalles sobre los diferentes tipos de alertas que admite Lighthouse.

Expandir tabla

Tipo de alerta	Valores disponibles durante la creación de la regla de alertas
Dispositivo no compatible	**Gravedad de la alerta:** Baja, Media, Alta, Informativa **Estado de cumplimiento:** No cumplimiento, En período de gracia, No evaluado **Tipo de dispositivo:** Desktop, Windows RT, Win MO6, Nokia, Windows Phone, Mac, Windows CE, Embedded Windows, iPhone, iPad, iPod, Android, SoC Consumer, Unix, Mac MDM, Windows HoloLens, Windows Surface Hub, Android (for work), Android (Enterprise), Windows 10x, Android (Google Mobile Services), Palm, Unknown
Dispositivos sin protección antivirus	**Gravedad de la alerta:** Baja, Media, Alta, Informativa **Protección contra amenazas:** Habilitado, Deshabilitado **Actualizaciones del antivirus:** Necesita actualizaciones
Detección de varianza	**Gravedad de la alerta:** Baja, Media, Alta, Informativa **Estado de implementación:** Incompleto, inelegible, erróneo
Usuario de riesgo	**Gravedad de la alerta:** Baja, Media, Alta, Informativa **Estado de riesgo:** En riesgo, confirmado en peligro
Registros de Windows	**Gravedad de la alerta:** Baja, Media, Alta, Informativa **Tipo de entrada:** Error, Advertencia, Información, Auditoría correcta, Auditoría de errores **Nombre del registro:** Todos los registros, Aplicación, Seguridad, Configuración, Sistema
Incidente de seguridad	**Gravedad de la alerta:** Baja, Media, Alta, Informativa **Clasificación:** No especificado, Falso positivo, Verdadero positivo, Positivo benigno **Determinación:** No especificado, Apt, Malware, Personal de seguridad, Pruebas de seguridad, Software no deseado, Otro, Ataque multiestado, Usuario en peligro, Phishing, Actividad de usuario malintencionado, Limpiar, Datos insuficientes, Actividad de usuario confirmada, Aplicación de línea de negocio **Origen del servicio:** No especificado, Microsoft Defender para punto de conexión, Microsoft Defender for Identity, Microsoft Defender para aplicaciones en la nube, Microsoft Defender para Office 365, Microsoft 365 Defender, Microsoft Entra Identity Protection, Microsoft App Governance, Prevención de pérdida de datos, Microsoft Defender for Cloud **Estado:** Todos, Desconocido, Nuevo, En curso, Resuelto
Comunicaciones de Lighthouse	**Gravedad de la alerta:** Baja, Media, Alta, Informativa **Eventos del sistema de Lighthouse:** Todos los eventos, disponibilidad de datos iniciales
Amenaza activa en el dispositivo	**Gravedad de la alerta:** Baja, Media, Alta, Informativa **Tipo de amenaza:** Todas las amenazas, Varios, Virus, Malware, Spyware

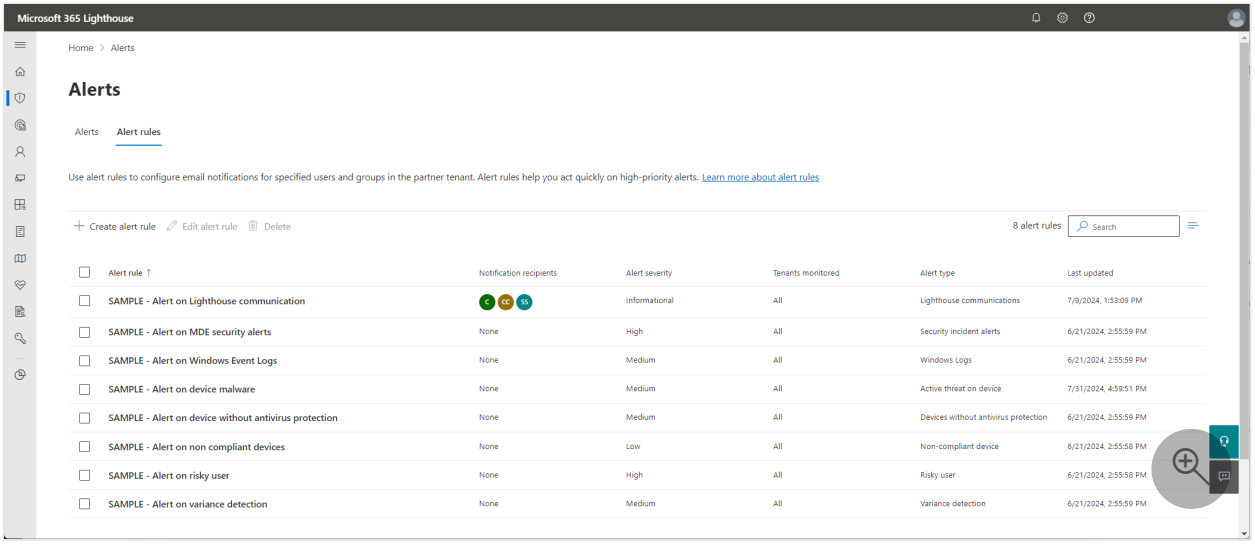
Tipo de alerta	Valores disponibles durante la creación de la regla de alertas
	Severidad: Desconocido, Bajo, Moderado, Alto, Grave

Pestaña Reglas de alerta

La pestaña **Reglas de alerta** muestra un resumen de todas las reglas de alerta del inquilino del asociado. Lighthouse proporciona ocho reglas de alerta predeterminadas que se aplican automáticamente a todos los clientes. Puede editar las reglas de alerta existentes o crear sus propias reglas de alertas personalizadas.

La pestaña **Reglas de alerta** también incluye las siguientes opciones:

- **Crear regla de alertas:** Seleccione esta opción para que Lighthouse le guíe por el proceso de creación de una regla de alertas personalizada.
- **Editar regla de alertas:** Seleccione esta opción para editar una regla de alertas existente.
- **Borrar:** Seleccione esta opción para eliminar una regla de alertas de la lista.
- **Buscar:** Escriba palabras clave para buscar una regla de alerta específica en la lista.



Contenido relacionado

Creación y administración de reglas de alertas (artículo)
Información general de la página Administración de amenazas en Microsoft 365 Lighthouse (artículo)
Mitigación de amenazas en Microsoft 365 Lighthouse con antivirus de Microsoft Defender (artículo)
Información general de la página Seguridad del dispositivo en Microsoft 365 Lighthouse (artículo)

Información general de la página Administración de vulnerabilidades en Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Creación y administración de reglas de alertas en Microsoft 365 Lighthouse

Artículo • 20/01/2025

Las reglas de alertas permiten configurar alertas de prioridad alta desde los siguientes servicios: Microsoft Defender para Empresas (MDB), Microsoft Defender Antivirus y Microsoft Entra ID.

Lighthouse proporciona un conjunto predeterminado de reglas de alerta basadas en procedimientos recomendados y recomendaciones. Puede usar estas reglas de alerta tal cual o modificarlas según sus preferencias y necesidades. También puede crear reglas de alerta personalizadas para obtener más control y flexibilidad.

Por ejemplo, puede crear una regla de alertas en Lighthouse para que le avise cuando se encuentre una amenaza activa en un dispositivo. Lighthouse comprueba las amenazas del servicio de Microsoft Defender para Empresas subyacente y, si se encuentra una amenaza activa, muestra una alerta en la página **Alertas** de Lighthouse. Lighthouse también envía una notificación de alerta por correo electrónico, si está configurado.

Para obtener más información sobre los diferentes tipos de alertas que puede crear, consulte Información general de la página Alertas de Microsoft 365 Lighthouse.

Antes de empezar

Debe tener el rol Administrador en Lighthouse para crear y administrar reglas de alertas.

Creación de una regla de alertas

> **Nota**
>
> Las alertas creadas en Lighthouse no se correlacionan con las alertas creadas en los portales de servicio subyacentes. Por ejemplo, si crea una alerta de Microsoft Defender para Empresas en Lighthouse, la misma alerta no se crea en el portal de Microsoft Defender.

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Alertas**.
2. En la página **Alertas** , seleccione la pestaña **Reglas de alerta** .
3. Seleccione **Crear regla de alertas**.

4. En la página **Configurar los conceptos básicos** , proporcione la siguiente información:

    - Nombre de la regla de alerta
    - Tipo de alerta
    - (Opcional) Descripción de la regla de alertas

5. Seleccione **Siguiente**.
6. En la página **Configuración** , configure las opciones de alerta. La configuración varía en función del tipo de alerta que seleccionó en la primera página.
7. Seleccione **Siguiente**.
8. En la página **Inquilinos** , seleccione qué inquilinos y etiquetas se van a supervisar.
9. En la página **Destinatarios** , seleccione quién debe recibir una notificación por correo electrónico cuando se desencadene la alerta. Puede enviar notificaciones a usuarios, grupos de seguridad o sistemas de vales.
10. Seleccione **Siguiente**.
11. Revise la información y, a continuación, seleccione **Guardar** para crear la regla de alertas.

Edición de una regla de alertas existente

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Alertas**.
2. En la página **Alertas** , seleccione la pestaña **Reglas de alerta** .
3. En la lista, seleccione una regla de alerta para editarla.
4. Seleccione **Editar regla de alertas**.
5. Recorra cada página y edite cualquier configuración según sea necesario.
6. Revise los cambios y, a continuación, seleccione **Guardar**.

Eliminación de una regla de alertas

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Alertas**.
2. En la página **Alertas** , seleccione la pestaña **Reglas de alerta** .
3. En la lista, seleccione una regla de alertas que desea eliminar.
4. Seleccione **Eliminar**.
5. En la ventana de confirmación, seleccione **Eliminar**.

Contenido relacionado

Información general de la página Alertas de Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Introducción a la información de Copilot en Microsoft 365 Lighthouse

Artículo • 08/11/2024

> **Nota**
>
> Estamos mejorando continuamente la información de Copilot. Háganos saber qué mejoras quiere que realicemos en esta característica para ayudarle a controlar y administrar el uso de Microsoft 365 Copilot proporcionando comentarios. En Lighthouse, seleccione el widget **Dar comentarios** en la esquina inferior derecha de cualquier página o vaya a la página Microsoft 365 Lighthouse comentarios.

Copilot Insights le ayuda a administrar y supervisar fácilmente Microsoft 365 Copilot éxito en los inquilinos de sus clientes, desde una sola página de **información de Copilot** en Lighthouse. Además de recomendar a los clientes que probablemente se beneficien de Copilot, en la página se muestran las asignaciones de uso y licencias de Copilot, la información de adopción de Copilot y los vínculos a recursos clave para ayudarle a convertirse en un experto de Copilot, incluido Copilot Lab, rutas de aprendizaje, vídeos de entrenamiento, las últimas actualizaciones de productos de Copilot, etc. La página también proporciona vínculos a los recursos que puede compartir con sus clientes para ayudarles a tener éxito con Copilot.

Acceso a la información de Copilot

Para acceder a los datos del cliente en la página **de conclusiones de Copilot** , debe configurar privilegios administrativos delegados granulares (GDAP) para cada cliente cuyos datos desea ver. Para más información, consulte Configuración de GDAP en Microsoft 365 Lighthouse.

Para ver la información del cliente en la pestaña **Oportunidades**, debe tener uno de los siguientes roles de Microsoft Entra en el inquilino del cliente:

- Administrador de licencias
- Lector global
- Administrador global

Para ver la información del cliente en la pestaña **Adopción**, debe tener uno de los siguientes roles de Microsoft Entra en el inquilino del cliente:

- Administrador de éxito de la experiencia del usuario
- Resumen de uso de Lector de informes
- Lector de informes
- Administrador de Teams
- Administrador de comunicaciones de Teams
- Administrador de Skype Empresarial
- Administrador de SharePoint
- Administrador de Exchange
- Lector global
- Administrador global

> ⊗ **Precaución**
>
> Para ayudar a proteger su organización, Microsoft recomienda usar roles con el nivel mínimo de permisos necesarios para realizar un trabajo. Administrador global es un rol con privilegios elevados que debe limitarse a escenarios en los que no se puede usar un rol con menos privilegios.

Oportunidades de Copilot

En el panel de navegación izquierdo de Lighthouse, seleccione **Copilot Insights** y, a continuación, seleccione la pestaña **Oportunidades** . En la parte superior de esta pestaña se muestra información general sobre cuántos de sus clientes pueden encontrar valor en Copilot. La pestaña también incluye una lista de inquilinos de clientes identificados como probables para encontrar valor en Copilot, junto con información adicional de Copilot relacionada con esos inquilinos. Estas conclusiones se basan en las señales de uso y licencia de Microsoft 365.

La lista de inquilinos incluye la siguiente información sobre cada inquilino:

- **Probabilidad**: probabilidad de que el cliente encuentre el valor en Microsoft 365 Copilot.
- **Licencias de requisitos previos de Copilot:** Número de licencias aptas para Copilot disponibles en el inquilino del cliente.
- **Identificado en:** Fecha en que se identificó por primera vez la oportunidad del cliente. Las recomendaciones se actualizan periódicamente para capturar las señales de cliente más recientes.

Adopción de Copilot

En el panel de navegación izquierdo de Lighthouse, seleccione **Copilot Insights** y, a continuación, seleccione la pestaña **Adopción** . Esta pestaña proporciona la siguiente información:

- **Tendencias de adopción:** Información sobre cómo han cambiado la habilitación de licencias de Copilot y el uso activo en todos los inquilinos de los clientes durante los últimos seis meses.
- **Recursos para usted:** Lista de recursos(incluidas rutas de aprendizaje, guías de adopción, tutoriales en vídeo, etc.) que puede compartir con sus clientes para ayudar a impulsar la interacción y aumentar su productividad mediante Copilot.

En la parte inferior de la pestaña **Adopción** hay una lista de inquilinos de clientes que tienen al menos una licencia de Microsoft 365 Copilot. La lista de inquilinos incluye la siguiente información sobre cada inquilino:

- **Velocidad de usuario activa:** Porcentaje de usuarios habilitados en el inquilino del cliente que fueron usuarios activos en el último mes. Para obtener más información sobre cómo se determina y notifica el uso de Copilot, consulte Interpretación del informe de uso de Microsoft 365 Copilot.
- **Licencias de Copilot:** Número total de licencias de Microsoft 365 Copilot en el inquilino del cliente.
- **Licencias sin asignar:** Número total de licencias de Microsoft 365 Copilot sin asignar en el inquilino del cliente.

Contenido relacionado

Introducción a Microsoft 365 Copilot (artículo)
requisitos de Microsoft 365 Copilot (artículo)
Habilitar usuarios para Microsoft 365 Copilot (artículo)
Información general de la página Acceso delegado en Microsoft 365 Lighthouse (artículo)
Configuración de GDAP en Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

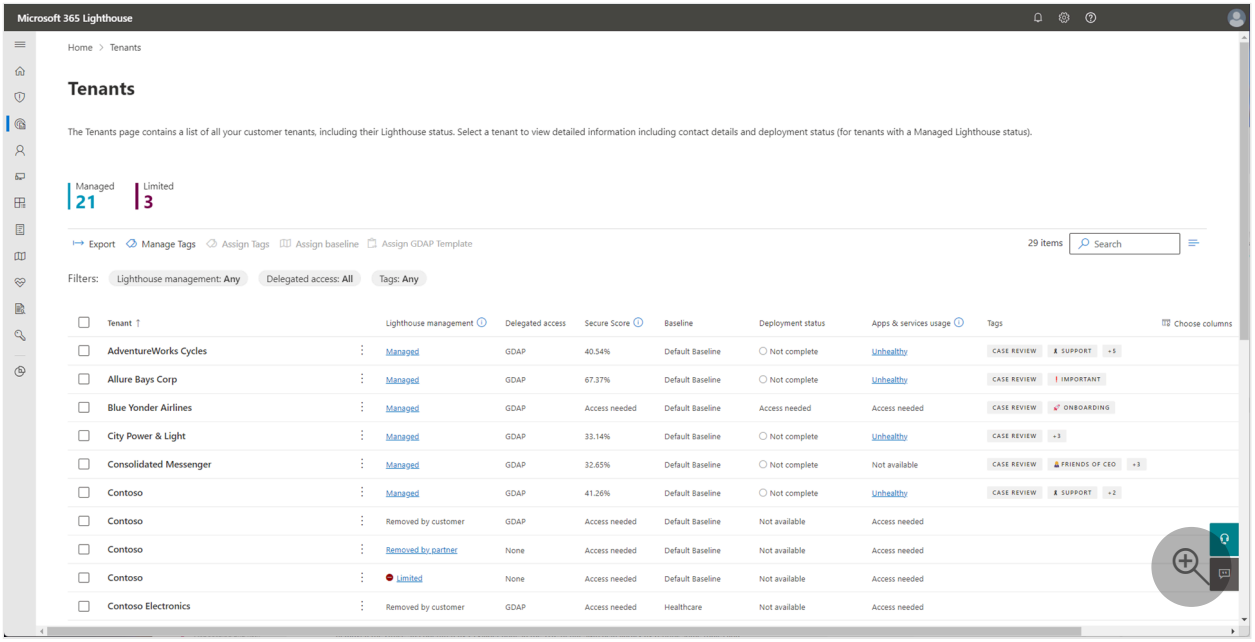
Información general de la página Inquilinos en Microsoft 365 Lighthouse

Artículo • 31/07/2024

Microsoft 365 Lighthouse le permite administrar cuentas de inquilinos de clientes seleccionando **Inquilinos** en el panel de navegación izquierdo para abrir la página **Inquilinos** . La página **Inquilinos** contiene una lista de todos los inquilinos del cliente. Puede seleccionar un inquilino para ver información detallada, incluidos los detalles de contacto y el estado de la implementación.

La página **Inquilinos** también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar datos de inquilino a un archivo de valores separados por comas (.csv) de Excel.
- **Administrar etiquetas:** Seleccione esta opción para agregar, editar o eliminar una etiqueta.
- **Asignar etiquetas:** Seleccione esta opción para asignar una etiqueta a un inquilino.
- **Asignar línea base:** Seleccione esta opción para asignar una línea base a un inquilino.
- **Buscar:** Escriba palabras clave para localizar rápidamente un inquilino específico en la lista.



Lista de inquilinos

La lista de inquilinos proporciona información sobre los distintos inquilinos de clientes con los que tiene un contrato, incluido su estado de administración de Lighthouse. La

lista de inquilinos también le permite etiquetar inquilinos para proporcionar diferentes filtros en Lighthouse, administrar servicios para inquilinos en el centro de administración aplicable y explorar en profundidad para obtener más información sobre un inquilino determinado y el estado de su plan de implementación.

Una vez que los inquilinos de los clientes cumplen los requisitos de incorporación de Lighthouse, su estado de administración de Lighthouse se mostrará como **Administrado** en la lista de inquilinos.

La lista de inquilinos le permite:

- Acceda a los centros de administración aplicables para administrar los servicios de los inquilinos del cliente.
- Ordene automáticamente los inquilinos por Administrado, Limitado, Quitado por asociado o Eliminado por cliente.
- Exporte la lista de inquilinos.
- Asignar y administrar etiquetas.
- Asigne una línea base.
- Busque inquilinos por nombre.
- Filtre los inquilinos por estado de administración de Lighthouse, acceso delegado o etiquetas.

Para quitar un inquilino, administrar servicios de inquilino o ver y administrar etiquetas, seleccione los tres puntos (más acciones) junto al nombre del inquilino. Puede ver inquilinos individuales seleccionando el nombre del inquilino o seleccionando una de las etiquetas asignadas al inquilino.

> **Sugerencia**
>
> También puede usar el filtro Inquilinos en la parte superior de cualquier página de Lighthouse para seleccionar un inquilino y, a continuación, acceder a los centros de administración aplicables para administrar los servicios de ese inquilino.

Para obtener información sobre cómo agregar inquilinos de cliente, consulte Agregar y administrar varios inquilinos en la cuenta del Centro de partners.

Estados

En la tabla siguiente se describen los distintos estados que puede ver en una o varias columnas para cada inquilino de cliente. Para obtener información sobre cómo

solucionar problemas de estados, consulte Solución de problemas y mensajes de error en Microsoft 365 Lighthouse: Incorporación de inquilinos del cliente.

Expandir tabla

Estado	Descripción
Acceso necesario	No tiene los privilegios de administrador delegado granular (GDAP) adecuados para ver la información. Póngase en contacto con un administrador del inquilino del asociado que pueda asignarle el rol GDAP adecuado para ver los datos en la página Inquilinos. Para ver qué roles GDAP proporcionan acceso a La puntuación de seguridad de Microsoft, consulte Puntuación de seguridad de Microsoft: permisos de roles globales de Microsoft Entra. Para ver qué roles de GDAP proporcionan acceso al uso de aplicaciones y servicios, consulte Informes de Microsoft 365 en el Centro de administración: Quién puede ver los informes.
Error	Se produjo un error durante el proceso de incorporación de este inquilino de cliente y estamos trabajando en una corrección. Si este error persiste durante más de 24 horas, póngase en contacto con el soporte técnico.
Limitado	Este inquilino de cliente solo tiene acceso a un conjunto limitado de experiencias en Lighthouse, incluida la configuración y administración de GDAP, la búsqueda de usuarios, los detalles del usuario, el etiquetado de inquilinos y el estado del servicio. Seleccione el nombre del inquilino para ver un estado detallado de los requisitos de administración de Lighthouse. Para obtener más información, consulte Requisitos para Microsoft 365 Lighthouse.
Administrados	Este inquilino de cliente se puede administrar y supervisar activamente en Lighthouse para usuarios y dispositivos con licencias necesarias.
No disponible	No hay datos disponibles para mostrar.
Quitado por el cliente	El cliente decidió no permitir el uso de Microsoft 365 Lighthouse para administrar su inquilino. Para permitir el uso de Microsoft 365 Lighthouse para administrar su inquilino, un administrador del inquilino del cliente debe ir a Configuración de la **organización** en el Centro de administración de Microsoft 365, seleccionar **Microsoft 365 Lighthouse** en la pestaña **Servicios** y, a continuación, seleccionar la opción para permitir el uso de experiencias de administración de clientes de Microsoft 365 Lighthouse en su inquilino.
Quitado por asociado	Su organización excluyó este inquilino de cliente de la administración de Lighthouse. Para reactivar el inquilino para la administración por Lighthouse, vaya a la página **Inquilinos** , seleccione los tres puntos (más acciones) junto al inquilino y, a continuación, seleccione **Administrar inquilino**.

> **Nota**
>
> Una vez que quite un inquilino de cliente, no podrá realizar ninguna acción en el inquilino hasta que se complete el proceso de eliminación. Este proceso puede tardar hasta 48 horas en completarse. Si decide volver a administrar el inquilino del cliente, los datos pueden tardar hasta 48 horas en volver a aparecer.

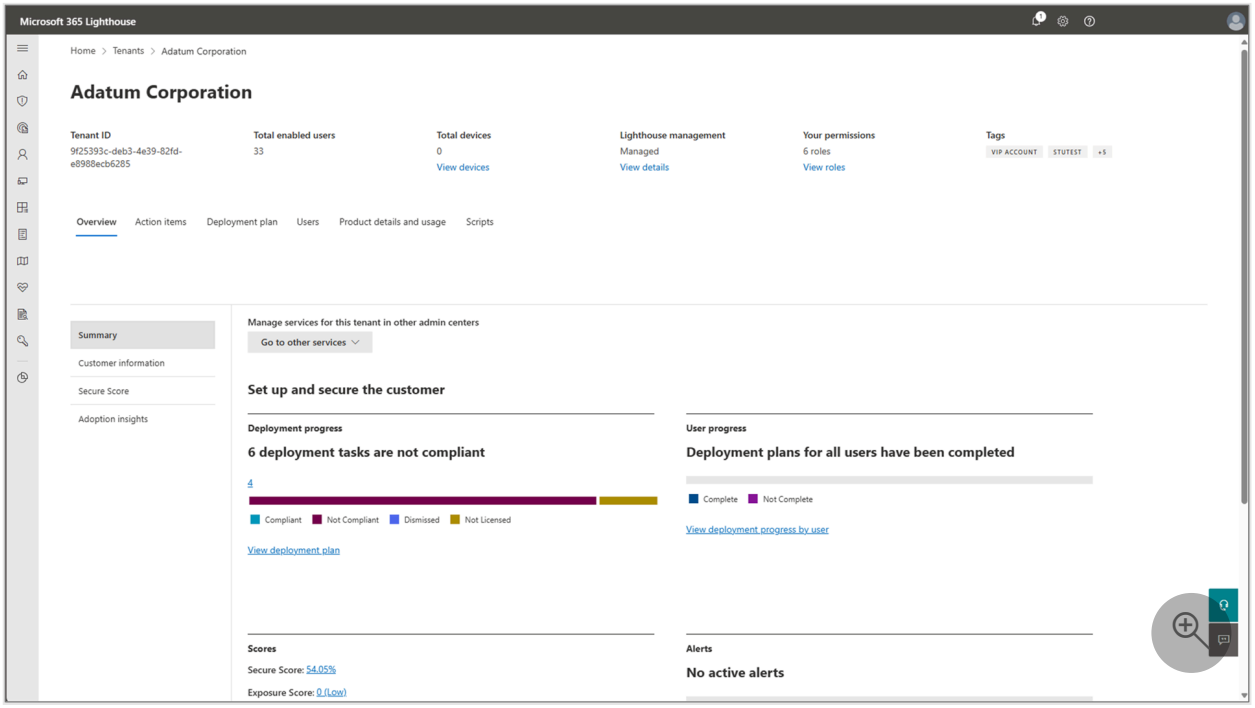
Etiquetas de inquilino

Para ayudar a organizar los inquilinos de los clientes y filtrar fácilmente las vistas existentes, puede crear y asignar etiquetas a los inquilinos. Para más información, consulte Administración de la lista de inquilinos en Microsoft 365 Lighthouse.

> **Nota**
>
> Puede crear hasta 30 etiquetas en todo el inquilino.

Página de detalles del inquilino

Para ver información detallada del inquilino del cliente, seleccione un inquilino en la lista de inquilinos. La página de detalles del inquilino contiene información de contacto y estado del plan de implementación.



Área de metadatos

El área de metadatos de la parte superior de la página proporciona información básica sobre el inquilino del cliente desde su cuenta de Microsoft 365.

Expandir tabla

Información del inquilino	Descripción
Identificación del inquilino	Identificador de inquilino de la organización.
Total de usuarios habilitados	Número de usuarios asignados en el inquilino del cliente.
Total de dispositivos	Número de dispositivos inscritos en el inquilino del cliente y administrados a través de Microsoft Intune. Seleccione **Ver dispositivos** para abrir la página **Dispositivos** para ver una lista de los dispositivos y la información de cumplimiento de dispositivos para el inquilino.
Administración de Lighthouse	Estado de administración del inquilino del cliente en Lighthouse: **Administrado**, **Limitado**, **Quitado por asociado** o **Eliminado por cliente**. Seleccione **Ver detalles** para abrir el panel de detalles de administración de Lighthouse para el inquilino.
Sus permisos	Número de roles asignados en el inquilino del cliente. Los roles determinan qué tareas puede completar para los clientes y qué datos puede ver. Seleccione **Ver roles** para abrir la página **Roles** para ver qué roles se le asignan en el inquilino.
Etiquetas	Etiquetas asignadas al inquilino del cliente en Lighthouse.

Pestaña da Información general

En la pestaña **Información general** , puede ver un resumen de información clave, información del cliente, puntuación segura, puntuación de exposición e información de adopción.

Resumen

La sección **Resumen** proporciona un resumen de alto nivel de información clave para el inquilino del cliente sobre el cumplimiento de línea base, la posición de seguridad y adopción, las alertas críticas y la información sobre las suscripciones del inquilino del cliente y el estado de almacenamiento del buzón.

Información del cliente

La sección **Información** del cliente proporciona un lugar para registrar información básica del cliente, como los planes de servicio en los que está el cliente y notas sobre el cliente para asegurarse de que todos los usuarios de su organización están en la misma página sobre la última interacción con el cliente.

Si su organización limita la frecuencia y quién puede ponerse en contacto directamente con los clientes, puede enumerar los administradores de involucración del cliente en esta pestaña para que otros usuarios de la organización sepan quién está autorizado para ponerse en contacto con el cliente.

Por último, puede usar esta pestaña para almacenar la información de contacto del cliente, incluido el nombre, el título, el teléfono, el correo electrónico y las notas sobre el contacto.

Puntuación de seguridad

La sección **Puntuación segura** proporciona información de puntuación segura de Microsoft sobre la organización del cliente para ayudarle a evaluar su posición de seguridad. La puntuación de seguridad de Microsoft es una medida de la posición de seguridad de una organización. Cuanto mayor sea la puntuación, mejor protegida será la organización frente a amenazas. Microsoft proporciona recomendaciones sobre cómo aumentar la puntuación de seguridad de una organización, lo que mejora su posición de seguridad. Para más información, consulte Puntuación de seguridad de Microsoft.

Conclusiones de adopción

La sección **Conclusiones de adopción** proporciona un subconjunto de la información de puntuación de adopción de Microsoft para la organización del cliente. La información de adopción le indica cómo la organización del cliente usa los productos y características de Microsoft para ayudarles a mejorar su productividad y a usar los productos de forma más eficaz. Para obtener más información, consulte Puntuación de adopción de Microsoft.

Pestaña Elementos de acción

La pestaña **Elementos de acción** muestra un resumen de los problemas clave del inquilino del cliente que requieren atención.

Dispositivos

En la sección **Dispositivos** se proporciona un resumen del número de problemas de dispositivo del cliente que requieren atención en todo el inquilino, incluido el cumplimiento, la protección contra amenazas, el estado del dispositivo, los problemas de Windows 365 y los registros de eventos de Windows. En esta sección también se proporcionan vínculos a las páginas asociadas donde puede ver detalles sobre los problemas.

Usuarios y correo electrónico

La sección **Usuarios y correo electrónico** le ayuda a evaluar rápidamente los problemas relacionados con usuarios de riesgo, la autenticación multifactor (MFA) y los mensajes en cuarentena.

Pestaña Plan de implementación

La pestaña **Plan de implementación** proporciona el estado del plan de implementación de un inquilino de cliente. Los pasos de implementación de la lista se basan en la línea base aplicada al inquilino. Para ver los detalles del paso de implementación, seleccione un paso de implementación de la lista.

La pestaña **Plan de implementación** también incluye las siguientes opciones:

- **Actualizar:** Seleccione esta opción para recuperar los datos del paso de implementación más actuales.
- **Buscar:** Escriba palabras clave para localizar rápidamente un paso de implementación específico en la lista.

Pestaña Usuarios

La pestaña **Usuarios** proporciona datos relevantes para los usuarios del inquilino del cliente.

Resumen

En la sección **Resumen** se proporciona información general sobre la información relacionada con los usuarios del inquilino del cliente, específicamente sobre el progreso de la tarea de implementación por parte del usuario y el estado de almacenamiento del buzón de cada usuario.

Progreso de la implementación

La sección **Progreso de la implementación** proporciona el estado de implementación de cada usuario para las tareas que admiten los informes de progreso del usuario. Seleccione cualquier usuario para ver más detalles. El progreso de la implementación solo está disponible para las tareas con licencia. El progreso del usuario solo se notifica para las tareas **compatibles,no compatibles** o **descartadas**.

La sección **Progreso de la implementación** también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar datos de inquilino a un archivo de valores separados por comas (.csv) de Excel.
- **Actualizar:** Seleccione esta opción para recuperar los datos del paso de implementación más actuales.
- **Buscar:** Escriba palabras clave para localizar rápidamente un paso de implementación específico en la lista.

Uso del buzón de correo

En la sección **Uso del buzón de correo** se proporcionan detalles sobre el estado de almacenamiento de los buzones de usuario y los buzones compartidos. En esta sección también se incluyen filtros que le ayudarán a administrar la lista de buzones, incluida la capacidad de identificar el estado de archivo de un buzón.

Pestaña Detalles y uso del producto

La pestaña **Detalles del producto y uso** contiene todos los datos relacionados con las suscripciones y el uso de licencias.

Uso de aplicaciones y servicios

La sección **Uso de aplicaciones y servicios** proporciona información sobre el uso de servicios de Microsoft 365, incluido el número de usuarios de un inquilino de cliente con licencia y uso activo de cada servicio.

En esta sección se incluye información sobre los siguientes servicios:

- **Servicios administrados en Microsoft 365 Lighthouse:** Estos servicios se pueden administrar en el portal de Lighthouse.
- **Servicios administrados en el Centro de administración de Microsoft 365:** Estos servicios se incluyen en la suscripción de Microsoft 365, pero no se pueden administrar en el portal de Lighthouse.

Dentro de las listas de servicios, la columna **Usuarios activos & dispositivos** indica el número de usuarios o dispositivos que iniciaron sesión en el servicio al menos una vez en los últimos 28 días. La columna **Cambio en la actividad** indica un cambio en los usuarios y dispositivos activos desde el mes pasado.

Lista de suscripciones

En la sección **Lista de suscripciones** se muestran todas las suscripciones que la organización vendió al cliente a través del canal proveedor de soluciones en la nube (CSP). La información del producto se limita a las suscripciones compradas a través de la nueva experiencia de comercio (NCE) y excluye las suscripciones de Azure.

Se captura la siguiente información para las suscripciones:

Expandir tabla

Información de suscripción	Descripción
Nombre del producto	Nombre de la suscripción.
Id. de suscripción	Número de identificador de la suscripción.
Estado	Estado de la suscripción: **Activo**, **Expirado** o **En gracia** (lo que significa que está en un período de gracia después de expirar y antes de que se cancele).
Fecha de finalización	Fecha de finalización de la suscripción.
Tipo	Si la suscripción es **de pago** o **de prueba**.
Facturación periódica	Si el cliente ha habilitado la suscripción para autorenew al final del período de suscripción.
Licencias de pago	Número de licencias de pago en la suscripción.
Frecuencia de facturación	Ciclo de facturación de la suscripción.
Canal de compra	Canal a través del cual se compró la suscripción.

Pestaña Scripts

La pestaña **Scripts** le permite crear e implementar scripts de PowerShell y comprobar los resultados de los scripts de los dispositivos administrados por Intune dentro del

inquilino del cliente.

Para obtener más información sobre cómo crear e implementar scripts de PowerShell, consulte Implementación de un script de PowerShell desde Microsoft 365 Lighthouse.

Contenido relacionado

Requisitos de Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Lighthouse de Microsoft 365 (artículo)
Administración de la lista de inquilinos en Microsoft 365 Lighthouse (artículo)
Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)
Puntuación de seguridad de Microsoft (artículo)
Puntuación de adopción de Microsoft (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Creación de un informe de cliente en Microsoft 365 Lighthouse

Artículo • 04/02/2025

Puede crear un informe PDF en Microsoft 365 Lighthouse para cada uno de los inquilinos del cliente que muestre el estado de su posición de seguridad junto con oportunidades para ayudarles a obtener el máximo valor de sus licencias existentes. El informe también resume las actividades que la organización asociada realizó en Lighthouse para mantener al cliente seguro, seguro y productivo. El informe está diseñado para compartirse con los clientes y puede ser especialmente útil durante las revisiones empresariales mensuales o trimestrales.

Antes de empezar

Para crear un informe de cliente, debe tener al menos el rol Lector global en Microsoft Entra ID para el inquilino del cliente. Para obtener más información, consulte Información general sobre los permisos en Microsoft 365 Lighthouse. Para obtener una lista completa de los roles Microsoft Entra y las acciones que pueden realizar, consulte Microsoft Entra roles integrados.

Creación de un informe de cliente

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. Seleccione un inquilino que muestre **Administrado** en la columna **Administración de Lighthouse** para abrir la página de detalles del inquilino para ese inquilino.
3. En la pestaña **Información general** , seleccione **Resumen** en el panel izquierdo y, a continuación, seleccione **Crear informe de cliente**.

   Se abre un panel de detalles que muestra información general de la información contenida en el informe.
4. Para crear y descargar una copia en PDF del informe, seleccione **Descargar PDF**.

> **Nota**
>
> Los datos de los informes de clientes se actualizan una vez a la semana.

Pasos siguientes

Después de descargar una copia en PDF del informe, puede recuperarla de la carpeta Descargas del equipo y compartirla con el cliente.

Contenido relacionado

Configuración de GDAP en Microsoft 365 Lighthouse (artículo)
Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Información general de la página Inquilinos de Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Ver los roles de Microsoft Entra en Microsoft 365 Lighthouse

Artículo • 20/01/2025

En este artículo se proporcionan instrucciones sobre cómo ver los roles de Microsoft Entra en los distintos inquilinos de clientes que administra su organización. El rol determina qué acciones puede realizar en Lighthouse.

Antes de empezar

Debe tener acceso a un inquilino de asociado que se haya incorporado al servicio Microsoft 365 Lighthouse.

Visualización de los roles

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. En la lista de inquilinos, seleccione cualquier nombre de inquilino para abrir la página de detalles del inquilino.
3. En **Sus permisos**, seleccione **Ver rol**.

   En la página **Roles** , si tiene uno o varios roles en un inquilino de cliente, verá una marca de verificación verde en la columna **Habilitado** para ese inquilino, junto con el número de roles que tiene. Si no tiene ningún rol en un inquilino, verá una **X** roja.
4. En el caso de los inquilinos de clientes con una marca de verificación verde junto a ellos, expanda el inquilino para ver la lista de roles que tiene en ese inquilino. Para obtener más información sobre los roles de Microsoft Entra y los permisos que conceden, consulte Microsoft Entra roles integrados.

   La página **Roles** también muestra las etiquetas personalizadas que se aplican a los inquilinos. Puede filtrar los datos de la página por roles o etiquetas asignados.

Pasos siguientes

Si no tiene permiso para realizar una acción que necesita realizar en Lighthouse, póngase en contacto con alguien que tenga el rol administrador en Lighthouse y pídale que le asigne un rol adecuado para la acción que intenta realizar.

Contenido relacionado

Introducción a los permisos en Microsoft 365 Lighthouse (artículo)
Administración de la lista de inquilinos en Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Administrar la lista de inquilinos en Microsoft 365 Lighthouse

Artículo • 24/09/2024

Para ayudarle a administrar la lista de inquilinos en Microsoft 365 Lighthouse, puede aplicar etiquetas personalizadas a los inquilinos. Estas etiquetas se pueden usar para organizar los inquilinos y también pueden ayudarle a filtrar las vistas existentes y la información disponible para los conjuntos de inquilinos pertinentes. Puede administrar las etiquetas desde la página **Inquilinos** . Una vez creadas y asignadas las etiquetas, puede ir a cualquier página de Lighthouse que tenga un filtro De inquilinos y usarlo para filtrar los datos en función de una etiqueta.

Antes de empezar

Debe ser administrador global en el inquilino del asociado.

Creación de una etiqueta

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. Seleccione **Administrar etiquetas**.
3. En el panel **Administrar etiquetas** , seleccione **Crear etiqueta**.
4. Escriba un nombre y una descripción opcional.
5. Haga clic en **Guardar**.

Edición de una etiqueta

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. Seleccione **Administrar etiquetas**.
3. En el panel **Administrar etiquetas** , seleccione los tres puntos (más acciones) junto a la etiqueta que desea editar y, a continuación, seleccione **Editar etiqueta**.
4. Edite el nombre, la descripción o los inquilinos asignados según sea necesario.
5. Haga clic en **Guardar**.

Asignación de una etiqueta a un inquilino

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. En la lista de inquilinos, seleccione los tres puntos (más acciones) junto al inquilino que desea etiquetar y, a continuación, seleccione **Etiquetas**.
3. Seleccione una etiqueta de la lista. Solo puede seleccionar una etiqueta a la vez.

   Las etiquetas que ya están asignadas al inquilino tienen una marca de verificación junto al nombre de la etiqueta.

Para asignar una etiqueta a varios inquilinos, active la casilla situada junto a cada inquilino de la lista que desea etiquetar, seleccione **Asignar etiquetas** y, a continuación, seleccione una etiqueta de la lista.

> **Nota**
>
> Puede crear hasta 30 etiquetas únicas y asignarlas a tantos inquilinos como sea necesario.

Eliminación de una etiqueta

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. Seleccione **Administrar etiquetas**.
3. En el panel **Administrar etiquetas** , seleccione los tres puntos (más acciones) junto a la etiqueta que desea eliminar y, a continuación, seleccione **Eliminar etiqueta**.
4. En el cuadro de diálogo de confirmación, seleccione **Confirmar**.

Eliminación de una etiqueta de un inquilino

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. En la lista de inquilinos, seleccione los tres puntos (más acciones) junto al inquilino que tiene una etiqueta que desea quitar y, a continuación, seleccione **Etiquetas**.
3. Seleccione la etiqueta que desea quitar.

   Las etiquetas que están asignadas actualmente al inquilino tienen una marca de verificación junto al nombre.

Para quitar una etiqueta de varios inquilinos, active la casilla situada junto a cada inquilino de la lista que tiene una etiqueta que desea quitar, seleccione **Asignar etiquetas** y, a continuación, seleccione una etiqueta activada en la lista.

Pasos siguientes

Después de crear y asignar etiquetas, puede usar esas etiquetas para filtrar los inquilinos. Vaya a cualquier página de Lighthouse que tenga un filtro Inquilinos, seleccione el filtro y, a continuación, escriba una etiqueta para filtrar por etiquetas o examinar y seleccione una o varias etiquetas de la lista. También puede crear nuevas etiquetas para admitir vistas específicas basadas en cada página.

Contenido relacionado

Información general de la página Inquilinos (artículo)
Ver los roles de Microsoft Entra en Microsoft 365 Lighthouse (artículo)
Visualización del estado del servicio de inquilino (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Visualización del estado del servicio de inquilino en Microsoft 365 Lighthouse

Artículo • 24/09/2024

Puede ver el estado del servicio de los inquilinos que administra en Microsoft 365 Lighthouse. Estado del servicio incluye incidentes y avisos para varios servicios, incluidos Microsoft Intune, Microsoft Entra servicios de identidad y servicios en la nube de administración de dispositivos móviles (MDM). También puede ver cuántos de los inquilinos administrados se ven afectados por incidentes. Por ejemplo, si uno de los inquilinos tiene problemas, puede comprobar la página de Estado del servicio para determinar si se trata de un problema conocido con una resolución en curso o si un cambio reciente podría afectar a ellos. Comprobar el estado del servicio podría ahorrarle tiempo para solucionar problemas y reducir las llamadas de soporte técnico.

Si no puede iniciar sesión en Lighthouse, puede usar la página Estado de mantenimiento del servicio de Microsoft para comprobar si hay problemas conocidos que le impidan iniciar sesión en el inquilino del asociado. Además, regístrese para seguir @MSFT365status en Twitter para ver información sobre incidentes de servicio específicos.

Antes de empezar

Para ver el estado del servicio, necesita un rol de Microsoft Entra en el inquilino del asociado con el siguiente conjunto de propiedades: **microsoft.office365.serviceHealth/allEntities/allTasks**. Para obtener una lista de Microsoft Entra roles, consulte Microsoft Entra roles integrados.

Ver el estado de mantenimiento del servicio y los detalles del problema

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Estado del servicio**.

2. En la parte superior de la página, revise el estado de mantenimiento del servicio actual de todos los inquilinos:

   - Número total de incidentes
   - Número total de avisos que afectan a cualquiera de los inquilinos administrados

- Número de servicios con incidentes activos

3. Para revisar los problemas por servicio, seleccione la pestaña **Todos los servicios** . Para revisar todos los problemas actuales, seleccione la pestaña **Todos los problemas** .

4. Seleccione un problema de la lista para abrir el panel de detalles del problema.

5. Seleccione la pestaña **Información general** para ver información como el tipo de problema, el estado, el impacto del usuario y el historial de problemas.

6. Seleccione la pestaña **Inquilinos afectados** para ver una lista de los inquilinos afectados por el problema. Desde aquí, puede exportar una lista de inquilinos afectados a un archivo de valores separados por comas (.csv) para que pueda compartirlo con los equipos de soporte técnico.

Contenido relacionado

Cómo comprobar el estado del servicio de Microsoft 365 (artículo)
Problemas conocidos con Microsoft 365 Lighthouse (artículo)
Ver los roles de Microsoft Entra en Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Implementación de un script de PowerShell desde Microsoft 365 Lighthouse

Artículo • 16/07/2024

Los scripts de PowerShell son archivos de texto sin formato que puede usar para automatizar procesos. Puede implementar scripts de PowerShell y comprobar los resultados de los scripts de los dispositivos administrados por Intune desde Lighthouse en lugar de tener que ir a la página Scripts de Microsoft Intune para cada inquilino de cliente.

Antes de empezar

Asegúrese de que los dispositivos de destino en los que ejecuta el script de PowerShell ejecutan Windows 10 o posterior (excepto Windows 10 Home) e inscritos en Intune.

Para obtener una lista detallada de los requisitos y obtener más información sobre el uso de scripts de PowerShell, consulte Uso de scripts de PowerShell en dispositivos Windows 10/11 en Intune.

Creación e implementación de un script de PowerShell

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos**.
2. En la lista de inquilinos, seleccione cualquier inquilino para abrir los detalles del inquilino.
3. Seleccione la pestaña **Scripts** y, a continuación, seleccione **Crear script**.
4. En la lista desplegable **Grupo de destino** , seleccione el grupo Microsoft Entra que se usará para dirigirse a los dispositivos en los que se ejecutará el script. El valor predeterminado es **Todos los dispositivos**.
5. En el cuadro **Título** , escriba un nombre para el script. Los nombres de script aparecen en la pestaña **Scripts** de Lighthouse y en el Centro de administración de Microsoft Intune .
6. (Opcional) Escriba una descripción del script.

7. En el cuadro **script de PowerShell** , escriba el script o cargue el archivo de script. El tamaño máximo del archivo es de 4 MB.

8. Seleccione **Implementar**.

Siguientes pasos

En la página **Scripts** de Lighthouse, seleccione el script de la lista para abrir los detalles del script. Desde aquí, puede ver una lista de dispositivos destinados a ejecutar el script y el estado del script. Tenga en cuenta que el script puede tardar algún tiempo en ejecutarse. Para obtener ayuda para solucionar problemas de scripts, consulte Problemas comunes y soluciones al usar scripts de PowerShell en dispositivos Windows 10/11 en Intune.

Contenido relacionado

Administración de grupos de Microsoft Entra y pertenencia a grupos (artículo)
Uso de scripts de PowerShell en dispositivos Windows 10/11 en Intune (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Información general de la página Usuarios de Microsoft 365 Lighthouse

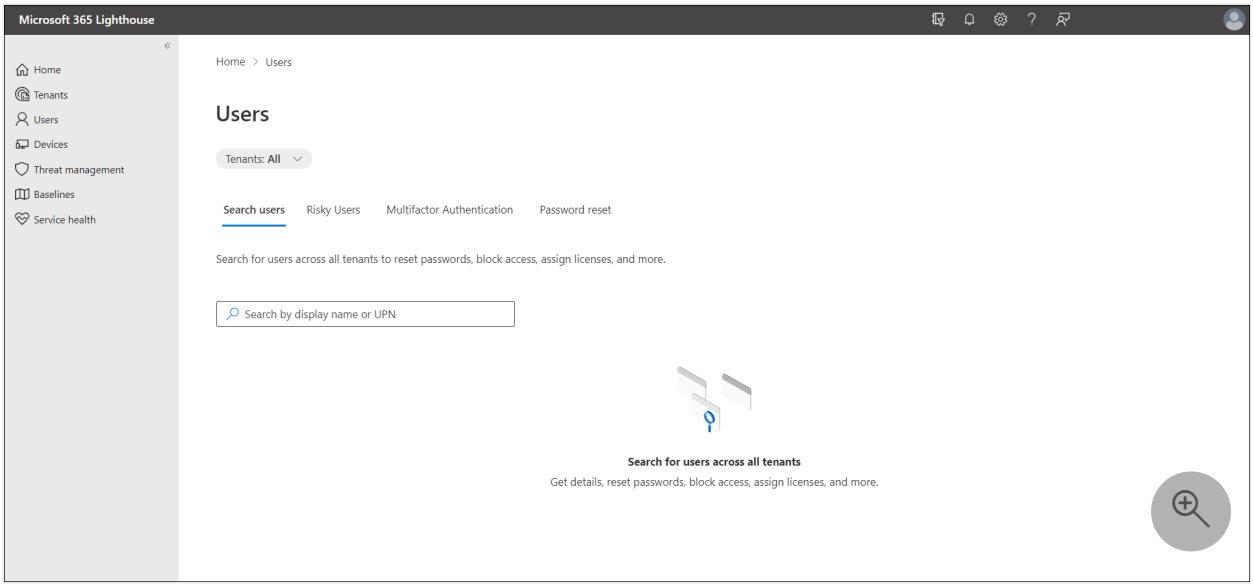
Artículo • 27/10/2023

Microsoft 365 Lighthouse permite administrar usuarios en cuentas de inquilino de clientes seleccionando cualquiera de los vínculos en **Usuarios** en el panel de navegación izquierdo. En la página Usuarios, puede buscar usuarios y evaluar y actuar sobre el estado de seguridad de las cuentas de usuario. También puede ver información sobre los usuarios de riesgo y el estado de la autenticación multifactor y el autoservicio de restablecimiento de contraseña (SSPR).

> **Nota**
>
> Estas páginas proporcionan información sobre los inquilinos para los que la disponibilidad de datos es limitada.

Página de administración de cuentas

En la página Administración de cuentas, puede buscar rápidamente usuarios específicos en los inquilinos y realizar tareas comunes de administración de usuarios, como actualizar la información de la cuenta de usuario, restablecer contraseñas, asignar licencias y administrar grupos, buzones de correo o OneDrive de un usuario. También puede ver cuentas inactivas, realizar las acciones de seguridad adecuadas y reclamar licencias sin usar.

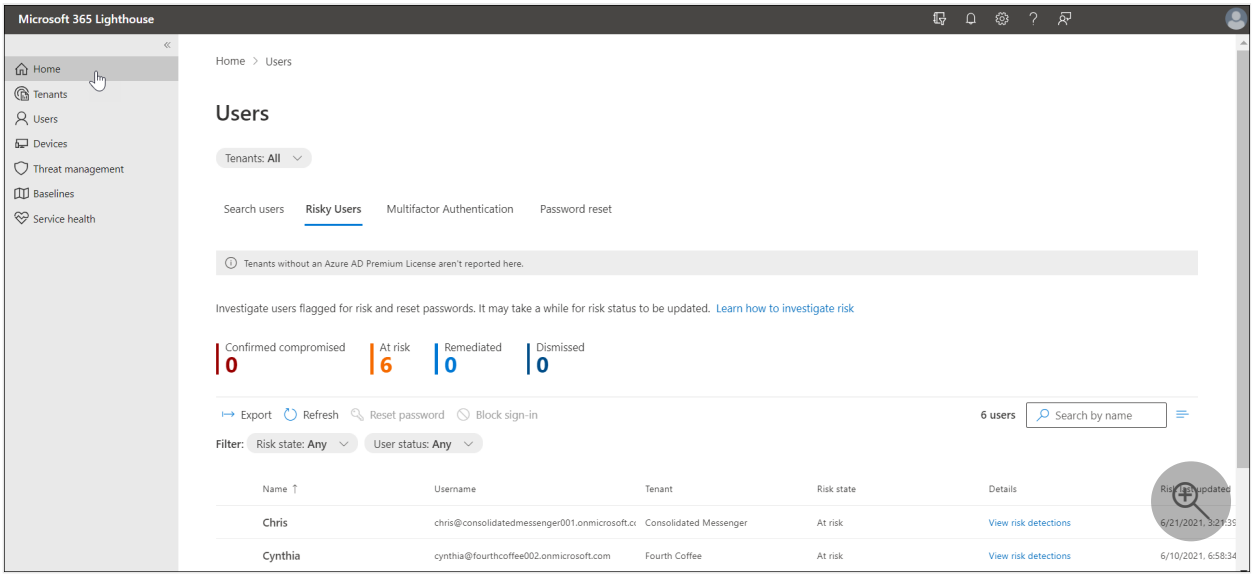


Página de usuarios de riesgo

En la página Usuarios de riesgo se muestran las cuentas de usuario de los inquilinos que se han marcado como comportamiento de riesgo. Seleccione cualquiera de los usuarios para ver más información sobre un riesgo detectado o para mitigar un riesgo mediante el restablecimiento de la contraseña de un usuario o el bloqueo del inicio de sesión. Para obtener más información sobre los tipos de riesgo y la detección, consulte ¿Qué es el riesgo?.

La página Usuarios de riesgo también incluye las siguientes opciones:

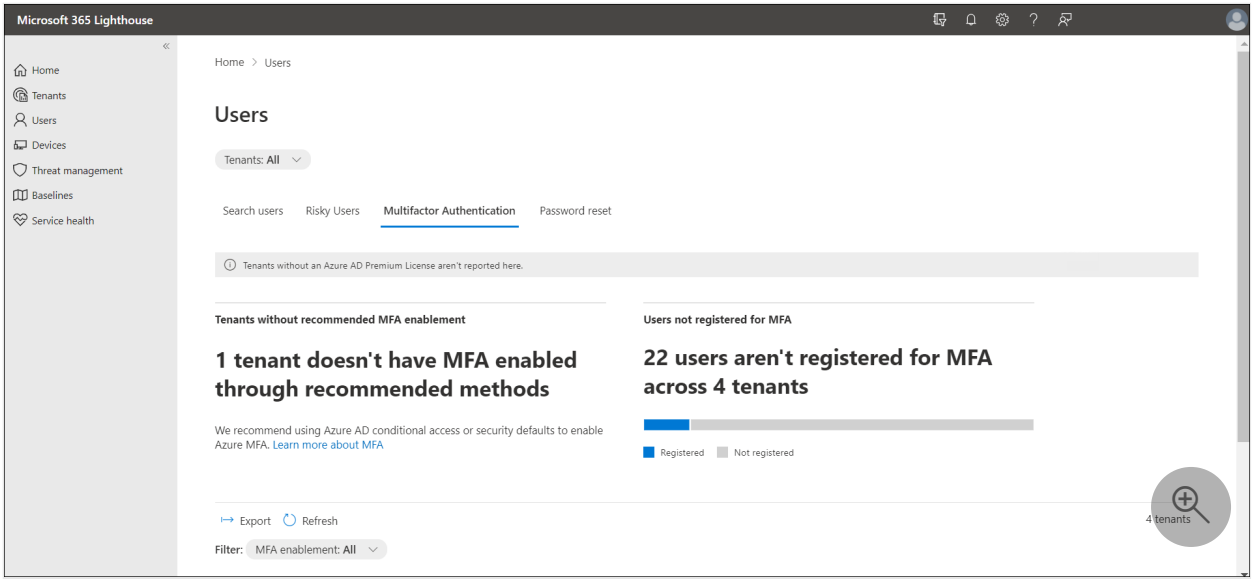
- **Exportar:** Seleccione esta opción para exportar los datos de cumplimiento de dispositivos a un archivo de valores separados por comas (.csv) de Excel.
- **Actualizar:** Seleccione esta opción para recuperar los datos de cumplimiento de dispositivos más actuales.
- **Confirme que los usuarios están en peligro:** Seleccione esta opción para confirmar que el usuario está en peligro.
- **Descartar el riesgo de los usuarios:** Seleccione esta opción para descartar el riesgo del usuario.
- **Restablecer contraseña:** Seleccione esta opción para cambiar o restablecer la contraseña de usuario.
- **Bloquear inicio de sesión:** Seleccione esta opción para evitar que nadie inicie sesión como este usuario.



Página Autenticación multifactor

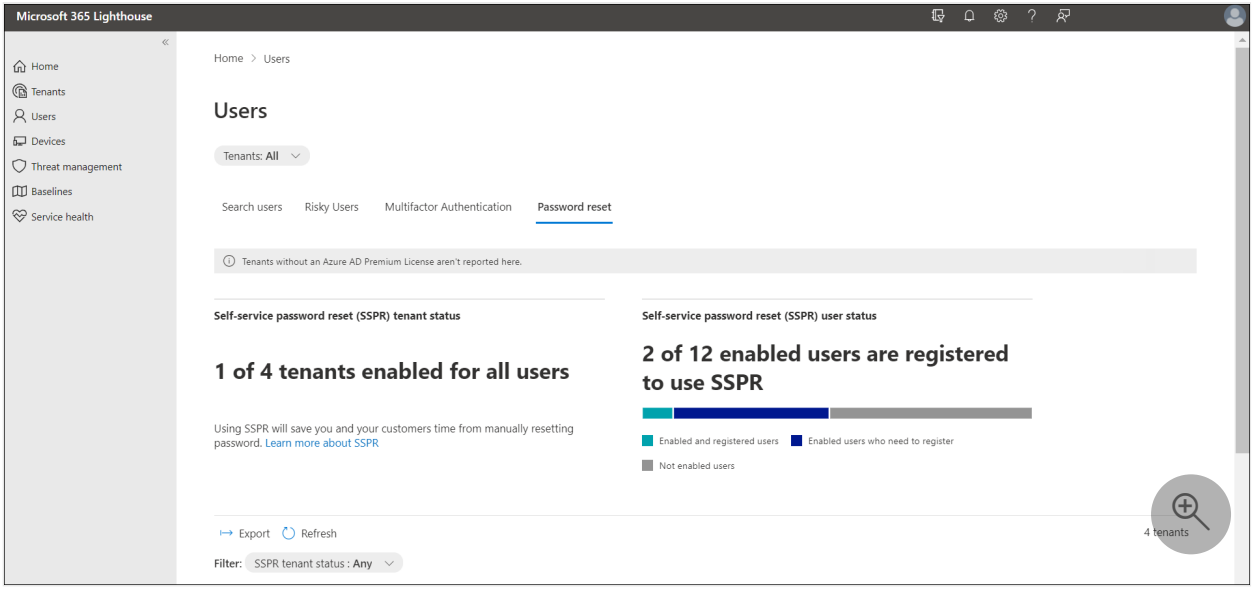
La página Autenticación multifactor proporciona información detallada sobre el estado de la habilitación de la autenticación multifactor (MFA) en los inquilinos. Seleccione cualquier inquilino de la lista para ver más detalles para ese inquilino, incluidas las

directivas de acceso condicional que requieren MFA ya configuradas y qué usuarios aún no se han registrado para MFA. Para obtener más información sobre MFA en Lighthouse, consulte Información general de la página autenticación multifactor.



Página de restablecimiento de contraseña

La página Restablecimiento de contraseña muestra información detallada sobre el estado de la habilitación de SSPR en los inquilinos. También proporciona información sobre los usuarios que tienen SSPR habilitado, pero que todavía necesitan registrarse para poder restablecer su contraseña por sí mismos.



Contenido relacionado

Información general de la página Autenticación multifactor (artículo)
Bloquear el inicio de sesión de usuario (artículo)

Bloquear el inicio de sesión para cuentas de buzón compartido (artículo)
Administración de usuarios inactivos (artículo)
Administración de la autenticación multifactor (artículo)
Administración del autoservicio de restablecimiento de contraseña (artículo)
Restablecer una contraseña de usuario (artículo)
Búsqueda de usuarios (artículo)
Visualización y administración de usuarios de riesgo (artículo)

Información general de la página Autenticación multifactor en Microsoft 365 Lighthouse

Artículo • 04/06/2024

La autenticación multifactor (MFA) en Microsoft Entra ID ayuda a proteger los inquilinos de los clientes frente a infracciones debido a credenciales perdidas o robadas mediante una segunda forma de autenticación para proporcionar una capa adicional de seguridad.

Hay varias maneras de habilitar MFA:

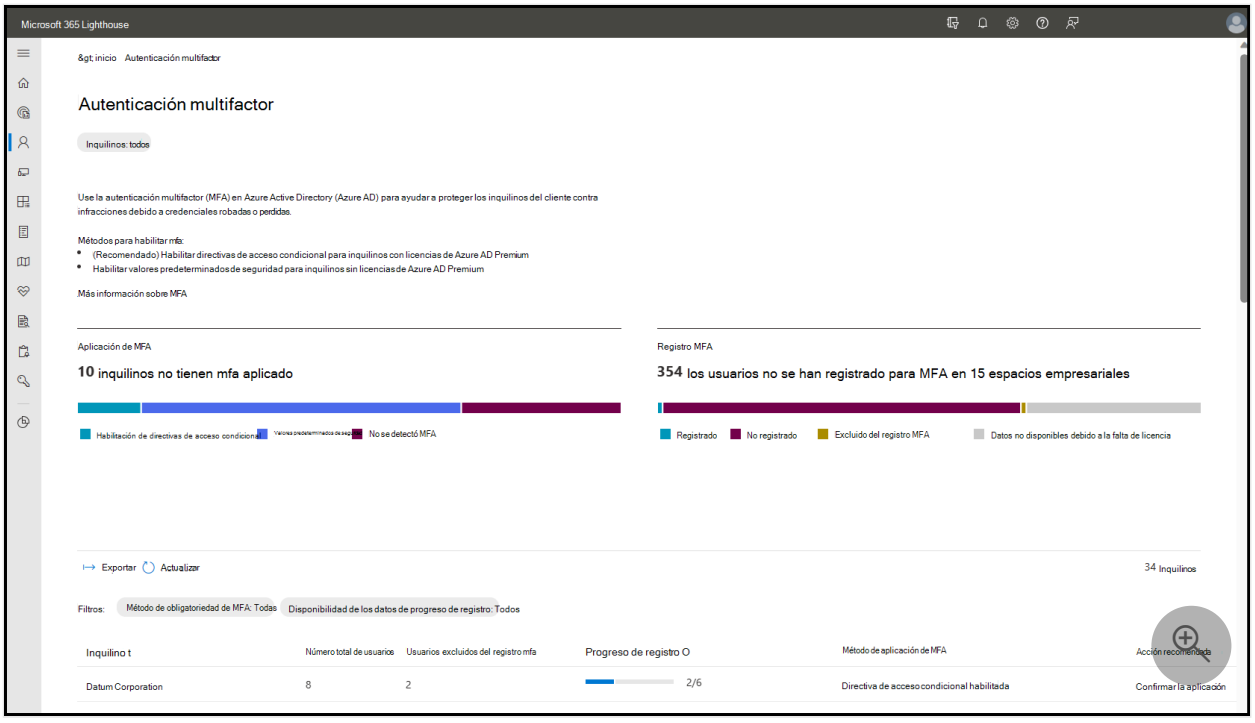
- **Directivas de acceso condicional (recomendado):** habilite las directivas de acceso condicional para inquilinos con licencias de Microsoft Entra ID P1 o P2.
- **Valores predeterminados de seguridad** : habilite los valores predeterminados de seguridad para los inquilinos sin licencias de Microsoft Entra ID P1 o P2.
- **MFA por usuario** : no se recomienda habilitar MFA por usuario a menos que el inquilino no tenga licencias de Microsoft Entra ID P1 o P2 y no quiera usar valores predeterminados de seguridad.

La página **Autenticación multifactor** proporciona información detallada sobre el estado de la habilitación de MFA en los inquilinos del cliente y las acciones recomendadas para mejorar la seguridad de los clientes. Seleccione cualquier inquilino de la lista para ver más detalles sobre ese inquilino, incluidas las directivas de acceso condicional que requieren MFA ya configuradas y los usuarios que todavía necesitan registrarse para MFA.

Página de autenticación multifactor

La página Autenticación multifactor incluye lo siguiente:

- Cumplimiento de MFA
- Registro de MFA
- Información de MFA
- Información de MFA por inquilino



Cumplimiento de MFA

El gráfico de cumplimiento de MFA mide el progreso de la aplicación de MFA por inquilino y notifica el estado de cumplimiento de MFA para cada inquilino como:

- **Habilitación de directivas de acceso condicional** : se habilitan una o varias directivas que requieren MFA.
- **Valores predeterminados de seguridad** : los valores predeterminados de seguridad están habilitados.
- **No se detectó MFA** : no hay directivas de acceso condicional que requieran MFA habilitadas y los valores predeterminados de seguridad se han deshabilitado.

> **Nota**
>
> La detección de una directiva de acceso condicional que requiere MFA con un estado de implementación habilitado no significa que todos los usuarios de destino deban autenticarse con MFA. Se necesita una evaluación de las directivas de acceso condicional de un inquilino en Microsoft 365 Lighthouse o en el Centro de administración de Microsoft Entra del inquilino para confirmar que el inquilino es seguro.

Registro de MFA

El gráfico de registro de MFA mide el progreso del registro de MFA por usuario y notifica el estado de registro de MFA para cada usuario como:

- **Registrado** : el usuario se ha registrado para MFA.
- **No registrado para MFA** : el usuario no se ha registrado para MFA.
- **Excluido de MFA** : el usuario se ha excluido del registro de MFA en Lighthouse.
- **Datos no disponibles debido a la falta de licencia** : el usuario es miembro de un inquilino para el que los datos no están disponibles debido a una licencia que falta.

> **Nota**
>
> La exclusión de un usuario del registro de MFA en Lighthouse no da lugar automáticamente a la exclusión del usuario de la tarea de implementación aplicable en Lighthouse ni de una directiva de acceso condicional configurada en el inquilino. Para asegurarse de que el usuario se excluye de la tarea de implementación aplicable en Lighthouse y de las directivas de acceso condicional configuradas en el inquilino, consulte Administración de la autenticación multifactor.

Información de MFA

La tabla de información de MFA se puede filtrar por el método de habilitación de MFA y la disponibilidad del progreso del registro de MFA.

La tabla proporciona la siguiente información para cada inquilino:

Expandir tabla

Columna	Descripción
Tenant	El nombre del inquilino.
Usuarios totales	Número de usuarios en el inquilino.
Usuarios excluidos del registro de MFA	Número de usuarios que se han excluido del registro de MFA en Lighthouse.
Progreso del registro	Número de usuarios no excluidos del registro de MFA en Lighthouse que se han registrado. **NOTA:** El número de usuarios registrados puede incluir usuarios excluidos del registro de MFA en Lighthouse.
Método de habilitación de MFA	Método de habilitación de MFA empleado por el inquilino.

Columna	Descripción
Acciones recomendadas	Las acciones que se recomiendan para optimizar la seguridad del inquilino.
Última actualización	Fecha en la que se actualizaron por última vez los datos.

Acciones recomendadas

Las acciones recomendadas se determinan para cada inquilino en función de la habilitación de MFA, las licencias y el progreso del registro.

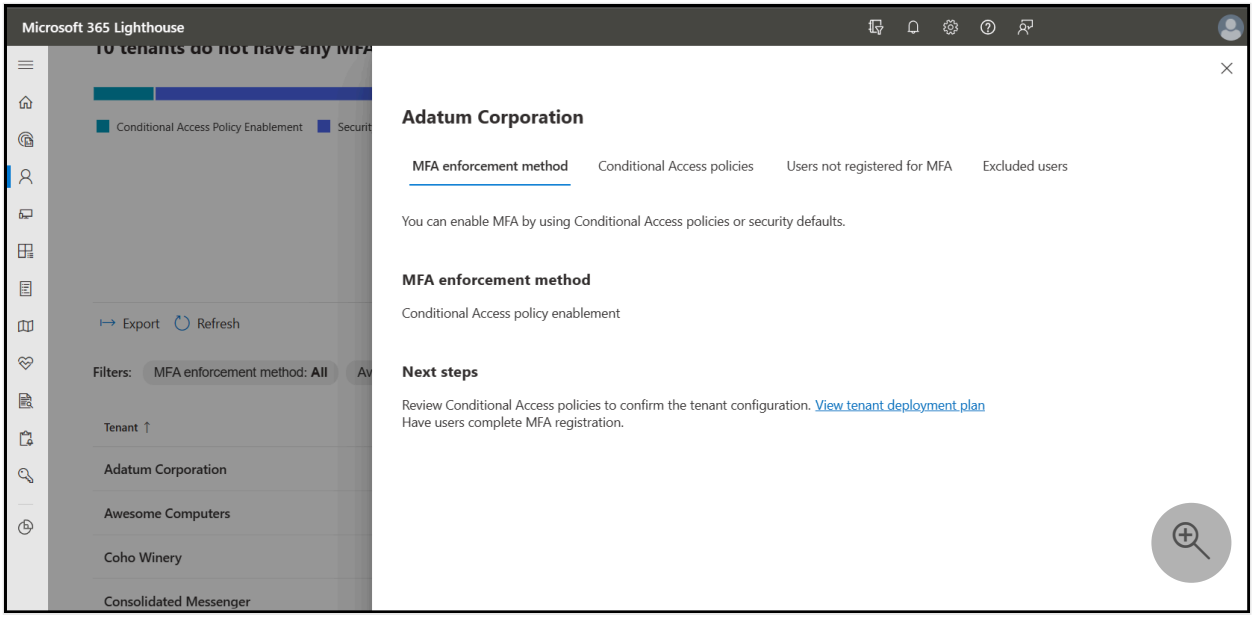
Expandir tabla

Habilitación de MFA	Licencias	Progreso del registro	Acciones recomendadas
Directiva de acceso condicional habilitada	Con Microsoft Entra ID P1 o P2	Completo	Evaluación de la implementación
		No completado	Evaluar la implementación, completar el registro de MFA
Valores predeterminados de seguridad	Con Microsoft Entra ID P1 o P2	Completo	Implementación del acceso condicional
		No completado	Implementación del acceso condicional, finalización del registro de MFA
	Sin el id. de entrada de Microsoft P1 o P2	Datos no disponibles debido a la falta de licencia	
No se detectó MFA	Con Microsoft Entra ID P1 o P2	Completo	Implementación del acceso condicional
		No completado	Habilitar valores predeterminados de seguridad, completar el registro de MFA
	Sin el id. de entrada de Microsoft P1 o P2	Datos no disponibles debido a la falta de licencia	

Información de MFA por inquilino

Al seleccionar cualquier inquilino de la lista, se abre el panel de detalles de MFA Insights para ese inquilino, que proporciona la siguiente información para cada inquilino:

- Método de habilitación de MFA
- Directivas de acceso condicional
- Usuarios no registrados para MFA
- Usuarios excluidos



Pestaña Método de habilitación de MFA

En la pestaña se proporcionan detalles específicos del inquilino sobre el método de habilitación de MFA del inquilino, vínculos a información adicional y los pasos siguientes que se deben realizar para optimizar la seguridad del inquilino.

Si el estado de habilitación de MFA del inquilino es **No se detectó MFA**, Lighthouse le pedirá que habilite los valores predeterminados de seguridad seleccionando el cuadro **Usar valores predeterminados de seguridad** .

Pestaña Directivas de acceso condicional

La pestaña enumera, vincula e informa del estado de cada directiva de acceso condicional detectada en el inquilino que requiere MFA. Puede usar los vínculos proporcionados para ver o editar la directiva detectada según sea necesario para optimizar la seguridad del inquilino.

Usuarios no registrados para la pestaña MFA

La pestaña proporciona las acciones recomendadas para administrar el registro de MFA y enumera las cuentas de usuario que ya se han habilitado para MFA, pero que aún necesitan registrarse con sus opciones de verificación permitidas para poder usar MFA.

Los usuarios no registrados para la tabla MFA pueden exportarse, actualizarse o filtrarse por administradores, miembros y usuarios invitados, y permite seleccionar cuentas de usuario para enviar correo electrónico, excluir o bloquear.

Pestaña Usuarios excluidos

En la pestaña se enumeran las cuentas de usuario que forman parte del grupo de seguridad **de exclusiones de Microsoft 365 Lighthouse - MFA** y que se han excluido del informe de MFA. Puede exportar y actualizar la lista y quitar usuarios de la lista de usuarios excluidos.

Contenido relacionado

Administración de la autenticación multifactor en Lighthouse (artículo)
Planeamiento de una implementación de autenticación multifactor de Microsoft Entra (artículo)
¿Qué son los valores predeterminados de seguridad? (artículo)
¿Qué es el acceso condicional? (artículo)
Obtenga información sobre cómo convertir usuarios de MFA por usuario a acceso condicional (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Bloquear el inicio de sesión de usuario Microsoft 365 Lighthouse

Artículo • 12/04/2024

Puede bloquear una cuenta de usuario si cree que está en peligro. Al bloquear una cuenta de usuario, impide inmediatamente que nadie inicie sesión en esa cuenta. Si un usuario intenta iniciar sesión, cerrará sesión automáticamente en todos los servicios de Microsoft 365 en un plazo de 60 minutos. El bloqueo de una cuenta de usuario no elimina ningún dato y no impide que la cuenta reciba correo.

Bloquear el inicio de sesión de un usuario

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Administración de cuentas** de **usuarios**> y, a continuación, seleccione la pestaña **Búsqueda usuarios**.
2. Escriba el nombre del usuario en el cuadro de búsqueda.
3. En la lista de resultados de búsqueda, seleccione el usuario.
4. En el panel de detalles del usuario, seleccione **Bloquear inicio de sesión**.
5. En el panel **Bloquear inicio de sesión** , seleccione **Bloquear el inicio de sesión de este usuario**.
6. Seleccione **Guardar cambios**.

Bloquear el inicio de sesión para usuarios de riesgo

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Usuarios**>**de riesgo**.
2. En la página **Usuarios de riesgo** , seleccione los usuarios que desea impedir que inicien sesión.
3. Seleccione **Bloquear inicio de sesión**.
4. En el panel **Administrar estado de inicio de sesión** , seleccione **Bloquear el inicio de sesión de los usuarios**.

5. Seleccione **Guardar**.

Contenido relacionado

Administración de cuentas de usuario de Microsoft 365 (artículo)
Restablecimiento de la contraseña de usuario (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Bloquear el inicio de sesión para cuentas de buzón compartido en Microsoft 365 Lighthouse

Artículo • 10/04/2024

Cada buzón compartido tiene una cuenta de usuario correspondiente. Un buzón compartido no está pensado para el inicio de sesión directo por su cuenta de usuario asociada. Siempre debe bloquear el inicio de sesión de la cuenta de buzón compartido y mantenerlo bloqueado.

Microsoft 365 Lighthouse proporciona visibilidad sobre todos los buzones compartidos en los inquilinos administrados que están habilitados para el inicio de sesión directo. Puede realizar un seguimiento y bloquear el inicio de sesión de todas las cuentas de buzón compartidos desde la pestaña **Buzones compartidos** de la página **Administración de** cuentas.

Bloquear el inicio de sesión para cuentas de buzón compartido

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Administración de cuentas** de **usuarios**> y, a continuación, seleccione la pestaña **Buzones compartidos**.
2. Seleccione la cuenta de buzón compartido que desea bloquear y, a continuación, seleccione **Bloquear inicio de sesión**.
3. En el panel **Administrar estado de inicio de sesión** , seleccione **Bloquear el inicio de sesión de los usuarios**.
4. Seleccione **Guardar**.

Notificar a los usuarios que el acceso está bloqueado (opcional)

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Administración de cuentas** de **usuarios**> y, a continuación, seleccione la pestaña **Buzones compartidos**.

2. Active la casilla situada junto a las cuentas de buzón compartido cuyo usuario desea notificar y, a continuación, seleccione **Crear correo electrónico**.

Lighthouse abre el cliente de correo electrónico predeterminado y rellena previamente el mensaje de correo electrónico para notificar a los usuarios seleccionados que su acceso de inicio de sesión se ha bloqueado.

Contenido relacionado

Bloquear el inicio de sesión de usuario (artículo)
Acerca de los buzones compartidos: administrador de Microsoft 365 (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Administración de usuarios inactivos en Microsoft 365 Lighthouse

Artículo • 24/09/2024

Microsoft 365 Lighthouse proporciona visibilidad sobre todos los usuarios de los inquilinos administrados que han estado inactivos durante más de seis meses. Las cuentas inactivas pueden presentar riesgos de seguridad y vincular licencias sin usar. En la pestaña **Usuarios inactivos** de la página **Administración** de cuentas, puede realizar un seguimiento de las cuentas inactivas y limpiarlas.

Lighthouse usa la actividad de inicio de sesión para detectar cuentas de usuario inactivas. La pestaña **Usuarios inactivos** muestra hasta 500 cuentas inactivas para cada inquilino.

Revisión de usuarios inactivos

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Administración de cuentasde usuarios**>.
2. En la página **Administración de** cuentas, seleccione la pestaña **Usuarios inactivos** y, a continuación, establezca los filtros para mostrar el resultado deseado.
3. En la lista de inquilinos, expanda cualquier inquilino para ver una lista de usuarios inactivos dentro del inquilino.
4. Seleccione cualquier usuario para abrir el panel de detalles del usuario y ver más información sobre la cuenta.
5. Una vez que determine que ya no se necesita una cuenta de usuario, puede eliminarla o bloquearla. Como mínimo, debe bloquear la cuenta de usuario para reducir los riesgos de seguridad. En el panel de detalles del usuario, seleccione **Bloquear inicio de sesión** o **Eliminar usuario**.

Bloquear el inicio de sesión para varias cuentas de usuario

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Administración de cuentasde usuarios**>.

2. En la página **Administración** de cuentas, seleccione la pestaña **Usuarios inactivos** y, a continuación, expanda cualquier inquilino de la lista para ver una lista de usuarios inactivos dentro del inquilino.

3. Seleccione los usuarios que desea bloquear y, a continuación, seleccione **Bloquear inicio de sesión**.

4. En el panel **Administrar estado de inicio de sesión** , seleccione **Bloquear el inicio de sesión de los usuarios**.

5. Seleccione **Guardar**.

Contenido relacionado

Administración de cuentas de usuario inactivas en Microsoft Entra ID (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Administración de la autenticación multifactor en Microsoft 365 Lighthouse

Artículo • 27/10/2023

Microsoft 365 Lighthouse permite administrar la configuración de autenticación multifactor (MFA) en todos los inquilinos. La página de autenticación multifactor proporciona información detallada sobre el estado de la habilitación de MFA y la capacidad de realizar acciones en usuarios específicos.

Para los clientes de pequeñas y medianas empresas (SMB), Microsoft recomienda habilitar los valores predeterminados de seguridad como mínimo. Para escenarios más complejos, puede usar el acceso condicional para configurar directivas específicas.

> **Nota**
>
> En esta página se proporciona información sobre los inquilinos para los que la disponibilidad de datos es limitada.

Antes de empezar

El inquilino del cliente debe estar activo dentro de Microsoft 365 Lighthouse. Para determinar si un inquilino está activo, consulte Microsoft 365 Lighthouse información general de la lista de inquilinos.

Notificar a los usuarios que no están registrados para MFA

1. En el panel de navegación izquierdo de Lighthouse, seleccione Autenticación**multifactorde usuarios**>.
2. Seleccione el inquilino que contiene los usuarios a los que desea notificar.
3. Seleccione **Usuarios no registrados para la pestaña MFA** .
4. Seleccione el inquilino que contiene los usuarios a los que desea notificar.
5. Seleccione **Crear correo electrónico**.

La aplicación de correo electrónico predeterminada crea un correo electrónico de ejemplo dirigido a cada usuario seleccionado.

6. Edite el correo electrónico de notificación si es necesario.
7. Envíe el correo electrónico.

> **Sugerencia**
>
> Seleccione los **recuentos de Administración**, **Invitado** o **Miembros** para filtrar la lista por tipo. Si las cuentas de usuario de la lista son cuentas de acceso de emergencia o de servicio para las que no desea requerir MFA, seleccione esas cuentas de usuario y, a continuación, seleccione **Excluir usuarios**. Las cuentas de usuario excluidas ya no aparecerán en la lista de usuarios no registrados para MFA.

> **Nota**
>
> Lighthouse abre el cliente de correo electrónico predeterminado y rellena previamente el mensaje de correo electrónico con instrucciones para registrarse en MFA. Todos los usuarios seleccionados se incluirán en la línea BCC. Si prefiere enviar un correo electrónico individualmente a los usuarios, puede seleccionar el icono de correo electrónico junto al nombre de usuario.
>
> Si desea usar una cuenta de correo electrónico diferente, puede exportar la lista de usuarios a un archivo. También puede descargar plantillas de correo electrónico de ejemplo que puede personalizar con la personalización de marca de su empresa.

Exclusión de usuarios del registro de MFA

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Autenticación multifactor de usuarios**>.
2. Seleccione el inquilino que contiene los usuarios que desea excluir.
3. Seleccione **Usuarios no registrados para la pestaña MFA** .
4. Seleccione los usuarios que desea excluir.
5. Seleccione **Excluir usuarios**.
6. En el panel **Excluir usuarios** , seleccione **Guardar cambios** para guardar los cambios en Lighthouse y en el inquilino.

> **Nota**
>
> Asegúrese de que el grupo de seguridad **Microsoft 365 Lighthouse - Exclusiones de MFA** está excluido de las directivas de acceso condicional del inquilino que requieren MFA y de las tareas de implementación aplicables en el plan de implementación del inquilino en Lighthouse.

Bloquear el inicio de sesión de los usuarios no registrados para MFA

1. En el panel de navegación izquierdo de Lighthouse, seleccione Autenticación**multifactorde usuarios**>.
2. Seleccione el inquilino que contiene los usuarios que desea bloquear.
3. Seleccione **Usuarios no registrados para la pestaña MFA** .
4. Seleccione los usuarios que desea bloquear.
5. Seleccione **Bloquear inicio de sesión**.
6. En el panel **Administrar estado de inicio de sesión** , seleccione **Bloquear el inicio de sesión de los usuarios**.
7. Haga clic en **Guardar**.

> **Nota**
>
> Asegúrese de que si aparecen cuentas de buzón de correo compartidas o cuentas de usuario inactivas en la lista de usuarios no registrados para MFA, se recomienda bloquear el inicio de sesión de esas cuentas para quitarlas de la lista.

El bloqueo de un usuario impide que alguien inicie sesión como este usuario y es una buena idea cuando cree que su contraseña o nombre de usuario pueden estar en peligro. El bloqueo de un usuario detiene inmediatamente los nuevos inicios de sesión de esa cuenta. La cuenta cerrará sesión automáticamente desde todos los servicios de Microsoft en un plazo de 60 minutos si la cuenta ha iniciado sesión. Esto no impedirá que la cuenta reciba correo y no elimina ningún dato de cuenta.

Eliminación de un usuario del grupo Usuarios excluidos

1. En el panel de navegación izquierdo de Lighthouse, seleccione Autenticación**multifactorde usuarios**>.

2. Seleccione el inquilino que contiene los usuarios que desea quitar.
3. Seleccione **la pestaña Excluir usuarios** .
4. Seleccione los usuarios que desea quitar.
5. Seleccione **Quitar**.
6. En el mensaje de confirmación, seleccione **Quitar**.

> ⓘ **Nota**
>
> Los usuarios excluidos que aparecen en Lighthouse reflejarán la pertenencia actual **Microsoft 365 Lighthouse grupo de seguridad de exclusiones de MFA**, pero no confirmarán que el grupo se ha excluido de las directivas de acceso condicional del inquilino que requieren MFA o de las tareas de implementación aplicables en el plan de implementación del inquilino en Lighthouse.

Pasos siguientes

Una vez habilitada mfa, puede habilitar Microsoft Entra autoservicio de restablecimiento de contraseña (SSPR). SSPR permite a los usuarios cambiar o restablecer contraseñas sin la intervención del administrador o del departamento de soporte técnico. Para obtener más información, vea Administrar el autoservicio de restablecimiento de contraseña en Microsoft 365 Lighthouse. Para obtener más información, vea Administrar el autoservicio de restablecimiento de contraseña en Microsoft 365 Lighthouse.

Contenido relacionado

Información general sobre la autenticación multifactor en Lighthouse (artículo)
Planear una implementación de autenticación multifactor Microsoft Entra (artículo)
¿Qué son los valores predeterminados de seguridad? (artículo)
¿Qué es el acceso condicional? (artículo)
Obtenga información sobre cómo convertir usuarios de MFA por usuario a acceso condicional (artículo)

Administración del autoservicio de restablecimiento de contraseña en Microsoft 365 Lighthouse

Artículo • 12/12/2023

Microsoft 365 Lighthouse permite a los proveedores de servicios administrados (MSP) administrar Microsoft Entra autoservicio de restablecimiento de contraseña (SSPR). SSPR ofrece a los usuarios la posibilidad de cambiar o restablecer su contraseña sin la participación del administrador o del departamento de soporte técnico. Si la cuenta de un usuario está bloqueada o olvida su contraseña, puede seguir las indicaciones para desbloquearse y volver a trabajar. Esta capacidad reduce las llamadas del departamento de soporte técnico y la pérdida de productividad cuando un usuario no puede iniciar sesión en su dispositivo o una aplicación.

La página Autoservicio de restablecimiento de contraseña proporciona información detallada sobre el estado de la habilitación de SSPR en los inquilinos del cliente y ayuda a garantizar que los usuarios están habilitados y registrados.

> ⓘ **Nota**
>
> En esta página se proporciona información sobre los inquilinos para los que la disponibilidad de datos es limitada.

Antes de empezar

Se debe cumplir la siguiente condición antes de que aparezca un inquilino en la lista:

- El inquilino del cliente debe estar activo en Lighthouse. Para obtener información sobre cómo determinar si un inquilino está activo, vea Información general de la página Inquilinos de Microsoft 365 Lighthouse.

Visualización del estado del inquilino de SSPR

En el panel de navegación izquierdo de Lighthouse, seleccione **Usuarios** > **Autoservicio de restablecimiento de contraseña**.

El módulo de estado de inquilino de SSPR notifica el estado de habilitación en todos los inquilinos de clientes que tienen una licencia Premium de Azure AD, informando de

cuántos inquilinos son:

- No habilitado para SSPR
- Habilitado para algunos usuarios
- Habilitado para todos los usuarios

Ver el estado de registro de usuario de SSPR

En el panel de navegación izquierdo de Lighthouse, seleccione **Usuarios** > **Autoservicio de restablecimiento de contraseña**.

La página Autoservicio de restablecimiento de contraseña proporciona información general sobre los inquilinos que han habilitado SSPR a través de la configuración recomendada, el número de usuarios que no se han registrado para SSPR y un desglose detallado por inquilino del progreso de la implementación de SSPR en las organizaciones que administra.

Ver los detalles del autoservicio de restablecimiento de contraseña

La tabla de detalles de autoservicio de restablecimiento de contraseña proporciona una vista detallada de la habilitación y el registro de SSPR para todos los inquilinos del cliente. La tabla se puede exportar, actualizar, buscar y filtrar por el estado del inquilino de SSPR, el estado de disponibilidad de SSPR y el progreso del registro de usuario. Los detalles del inquilino notificados en la tabla incluyen:

Expandir tabla

Columna	Descripción
Tenant	El nombre del inquilino.
Usuarios totales	Número de usuarios en el inquilino.
Usuarios habilitados	Número de usuarios habilitados para SSPR.
Progreso del registro	Número total de usuarios que se han registrado para SSPR.

> **Nota**
>
> Los usuarios habilitados y los datos de progreso del registro no estarán disponibles para los inquilinos que no tengan una licencia premium Microsoft Entra.

Al seleccionar cualquier inquilino en la tabla de detalles de autoservicio de restablecimiento de contraseña, se abre el panel de detalles del inquilino, que proporciona detalles adicionales sobre el estado de habilitación y registro de usuario del inquilino.

Habilitación de SSPR para un inquilino

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Usuarios**>**Autoservicio de restablecimiento de contraseña**.
2. En la página **Autoservicio de restablecimiento de contraseña** , seleccione un inquilino de la lista para abrir el panel de detalles.
3. Seleccione **Editar configuración de SSPR en Azure Active Directory** para ir a Azure Active Directory (Azure AD).
4. En Azure AD, habilite SSPR para todos los usuarios o seleccionados. Para más información, consulte Tutorial: Permitir que los usuarios desbloqueen su cuenta o restablezcan contraseñas mediante el autoservicio de restablecimiento de contraseña de Azure Active Directory.

Notificar a los usuarios que se registren para SSPR

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Usuarios**>**Autoservicio de restablecimiento de contraseña**.
2. En la página **Autoservicio de restablecimiento de contraseña** , seleccione un inquilino de la lista para abrir el panel de detalles.
3. Seleccione los usuarios a los que desea notificar.
4. Seleccione **Crear correo electrónico**.

Lighthouse abre el cliente de correo electrónico predeterminado y rellena previamente el mensaje de correo electrónico con instrucciones para registrarse en SSPR. Todos los usuarios seleccionados se incluyen en la línea BCC. Si prefiere enviar un correo electrónico individualmente a los usuarios, puede seleccionar el icono de correo electrónico junto al nombre de usuario.

Si desea usar una cuenta de correo electrónico diferente, puede exportar la lista de usuarios a un archivo. También puede descargar plantillas de correo electrónico de

ejemplo que puede personalizar con la personalización de marca de la empresa.

Contenido relacionado

Planeamiento de una implementación de autoservicio de restablecimiento de contraseña de Microsoft Entra (artículo)
Tutorial: Permitir que los usuarios desbloqueen su cuenta o restablezcan contraseñas mediante Microsoft Entra autoservicio de restablecimiento de contraseña (artículo)
Habilitación y configuración de SSPR en Microsoft Entra id. (vídeo)
Administración de la autenticación multifactor en Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Restablecer una contraseña de usuario en Microsoft 365 Lighthouse

Artículo • 03/10/2024

Microsoft 365 Lighthouse permite cambiar o restablecer contraseñas de usuario. Puede restablecer la contraseña de uno o varios usuarios o usuarios de riesgo en los mismos inquilinos o en otros.

Restablecimiento de una contraseña para uno o varios usuarios

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Administración de cuentasde usuarios**>.
2. En la pestaña **Buscar usuarios** , escriba todo o parte del nombre del usuario en el cuadro de búsqueda y presione **Entrar**.
3. En la lista de resultados de búsqueda, active la casilla situada junto a uno o varios usuarios de la lista y, a continuación, seleccione **Restablecer contraseña**.
4. En el panel **Restablecer contraseña** , seleccione **Generar automáticamente la contraseña** o **Permitirme crear una contraseña**. Si decide crear una contraseña, escriba una contraseña en el cuadro **Contraseña** (la contraseña será la misma para todos los usuarios seleccionados).
5. Si desea que los usuarios cambien su contraseña después del primer inicio de sesión, seleccione **Requerir que estos usuarios cambien su contraseña cuando inicien sesión por primera vez**.
6. Seleccione **Restablecer contraseña**.

Restablecimiento de una contraseña para uno o varios usuarios de riesgo

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Usuarios**>**de riesgo**.
2. En la página **Usuarios de riesgo** , active la casilla situada junto a uno o más usuarios de riesgo en la lista y, a continuación, seleccione **Restablecer contraseña**.

3. En el panel **Restablecer contraseña** , seleccione **Generar automáticamente la contraseña** o **Permitirme crear una contraseña**. Si decide crear una contraseña, escriba una contraseña en el cuadro **Contraseña** (la contraseña será la misma para todos los usuarios seleccionados).

4. Si desea que los usuarios cambien su contraseña después del primer inicio de sesión, seleccione **Requerir que estos usuarios cambien su contraseña cuando inicien sesión por primera vez**.

5. Seleccione **Restablecer contraseña**.

Contenido relacionado

Administración de cuentas de usuario de Microsoft 365 (artículo)
Bloquear el inicio de sesión de usuario Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Buscar usuarios en Microsoft 365 Lighthouse

Artículo • 22/10/2024

Microsoft 365 Lighthouse permite buscar un usuario específico en todos los inquilinos activos. Esto le permite encontrar un usuario rápidamente sin necesidad de navegar por diferentes inquilinos.

1. En el panel de navegación izquierdo de Lighthouse, seleccione**Administración de cuentasde usuarios**>.
2. En la pestaña **Buscar usuarios** , escriba todo o parte de un nombre para mostrar o un nombre principal de usuario (UPN) en el cuadro de búsqueda.
3. En la lista de resultados de búsqueda, seleccione un usuario para abrir el panel de detalles del usuario.

Pasos siguientes

Una vez que se encuentra el usuario, puede restablecer su contraseña, bloquear su cuenta o eliminar su cuenta. Para obtener más información, vea Restablecer contraseña de usuario o Bloquear inicio de sesión de usuario Microsoft 365 Lighthouse.

Contenido relacionado

Administración de cuentas de usuario de Microsoft 365 (artículo)
Restablecer una contraseña de usuario en Microsoft 365 Lighthouse (artículo)
Bloquear el inicio de sesión de usuario Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Visualización y administración de usuarios de riesgo en Microsoft 365 Lighthouse

Artículo • 13/11/2024

Microsoft recopila y analiza billones de señales de inicio de sesión de usuario cada día. Estas señales se usan para ayudar a crear buenos patrones de comportamiento de inicio de sesión de usuario e identificar posibles intentos de inicio de sesión de riesgo. Protección de Microsoft Entra ID usa estas señales para revisar los intentos de inicio de sesión de usuario y tomar medidas si hay actividad sospechosa.

Microsoft 365 Lighthouse ayuda a administrar los riesgos detectados por Protección de Microsoft Entra ID proporcionando una vista única de los usuarios de riesgo en todos los inquilinos administrados. Para proteger rápidamente a los usuarios de riesgo, restablezca su contraseña o bloquee el inicio de sesión en su cuenta de Microsoft 365. También puede ver información para comprender mejor el riesgo de un usuario y determinar los pasos siguientes.

Protección de Microsoft Entra ID identifica los riesgos de muchos tipos, entre los que se incluyen:

- Credenciales filtradas
- Uso de IP anónima
- Viaje atípico
- Inicio de sesión desde dispositivos infectados
- Inicio de sesión desde direcciones IP con actividad sospechosa
- Inicio de sesión desde ubicaciones desconocidas

> ⓘ **Nota**
>
> En esta página se proporciona información sobre los datos que están limitados o no están disponibles debido a licencias insuficientes.

Antes de empezar

Se deben cumplir las condiciones siguientes para que los usuarios puedan aparecer en la lista de usuarios de riesgo:

- El inquilino del cliente debe tener una licencia P1 o P2 de Microsoft Entra ID para cada usuario. Para obtener más información sobre qué licencias admiten Protección de Microsoft Entra ID, consulte ¿Qué es Identity Protection?
- El inquilino del cliente debe estar activo dentro de Microsoft 365 Lighthouse. Para determinar si un inquilino está activo, consulte Información general de la página Windows 365 (PC en la nube) en Microsoft 365 Lighthouse.

Revisar los riesgos detectados y tomar medidas

En Protección de Microsoft Entra ID, las detecciones de riesgos incluyen las acciones sospechosas identificadas relacionadas con las cuentas de usuario en Microsoft Entra ID.

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Usuarios**>**de riesgo**.
2. En la página **Usuarios de riesgo** , revise los usuarios de la lista con un estado de riesgo **de En riesgo**.
3. Seleccione **Ver detecciones de riesgos** para obtener información detallada sobre los riesgos detectados para cada usuario. Para obtener más información sobre los tipos de riesgo y la detección, consulte ¿Qué es el riesgo?.
4. Para cada usuario, evalúe las detecciones de riesgo y seleccione una de las siguientes acciones, según corresponda:
    - Restablecer contraseña: cambie o restablezca la contraseña de usuario.
    - Bloquear inicio de sesión: impedir que nadie inicie sesión como este usuario.
    - Confirmar que el usuario está en peligro: establezca el estado de riesgo en confirmado en peligro.
    - Descartar el riesgo de usuario: establezca el estado de riesgo en descartado.

Realizar acciones en varias cuentas de usuario a la vez

Para realizar acciones en varios usuarios afectados a la vez:

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Usuarios**>**de riesgo**.

2. En la página **Usuarios de riesgo** , seleccione el conjunto de usuarios en los que desea realizar acciones.

3. Elija una de las siguientes acciones para realizar:

    - Restablecer contraseña
    - Bloquear inicio de sesión
    - Confirmar que el usuario está en peligro
    - Descartar el riesgo del usuario

> **Nota**
>
> Si una organización que administra tiene una licencia Microsoft Entra ID P2, se recomienda habilitar las directivas de acceso condicional basadas en riesgos de usuario para esa organización. Para obtener más información, vea Acceso condicional: Acceso condicional basado en riesgos del usuario.

Contenido relacionado

Usar detecciones de riesgo para inicios de sesión de usuario para desencadenar Microsoft Entra cambios de contraseña o autenticación multifactor (tutorial)
¿Qué es el riesgo? (artículo)
Corrección de riesgos y desbloqueo de usuarios (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Información general de la página Estado del dispositivo en Microsoft 365 Lighthouse

Artículo • 08/11/2023

Microsoft 365 Lighthouse incluye las características de Análisis de puntos de conexión de Microsoft para dispositivos en una vista simplificada de administración multiinquilino. Los problemas de rendimiento y otros problemas pueden pasar desapercibidos por un inquilino durante un período prolongado, lo que afecta a la experiencia del usuario final y aumenta los costos de soporte técnico. La página Estado del dispositivo aporta estos problemas a la superficie más rápido y en varios inquilinos para ahorrar tiempo y dolor al usuario final, ya que le permite obtener información y solucionar problemas.

La página Estado del dispositivo proporciona un subconjunto de análisis de dispositivos que se ofrecen mediante análisis de puntos de conexión, en concreto, procesos de inicio y rendimiento del dispositivo. Los datos de ejemplo incluyen el estado de mantenimiento del dispositivo, los reinicios totales, las pantallas azules totales, los procesos superiores y las especificaciones de hardware. Los datos solo reflejan dispositivos Windows totalmente administrados. No se admiten los datos de Bring Your Own Devices.

> ⓘ **Nota**
>
> En esta página se proporciona el número de inquilinos para los que los datos no están disponibles porque no tienen las licencias necesarias.

Requisitos

Los dispositivos deben inscribirse en Microsoft Intune. Para obtener más información sobre la inscripción, consulte ¿Qué es Análisis de puntos de conexión? Una vez inscrito un dispositivo, la página Estado del dispositivo se rellena automáticamente con datos. Las actualizaciones pueden tardar hasta 48 horas.

> ⓘ **Nota**
>
> Si los datos no aparecen para un inquilino específico, compruebe que la directiva está habilitada. En el plan de implementación del inquilino, en **Configurar la**

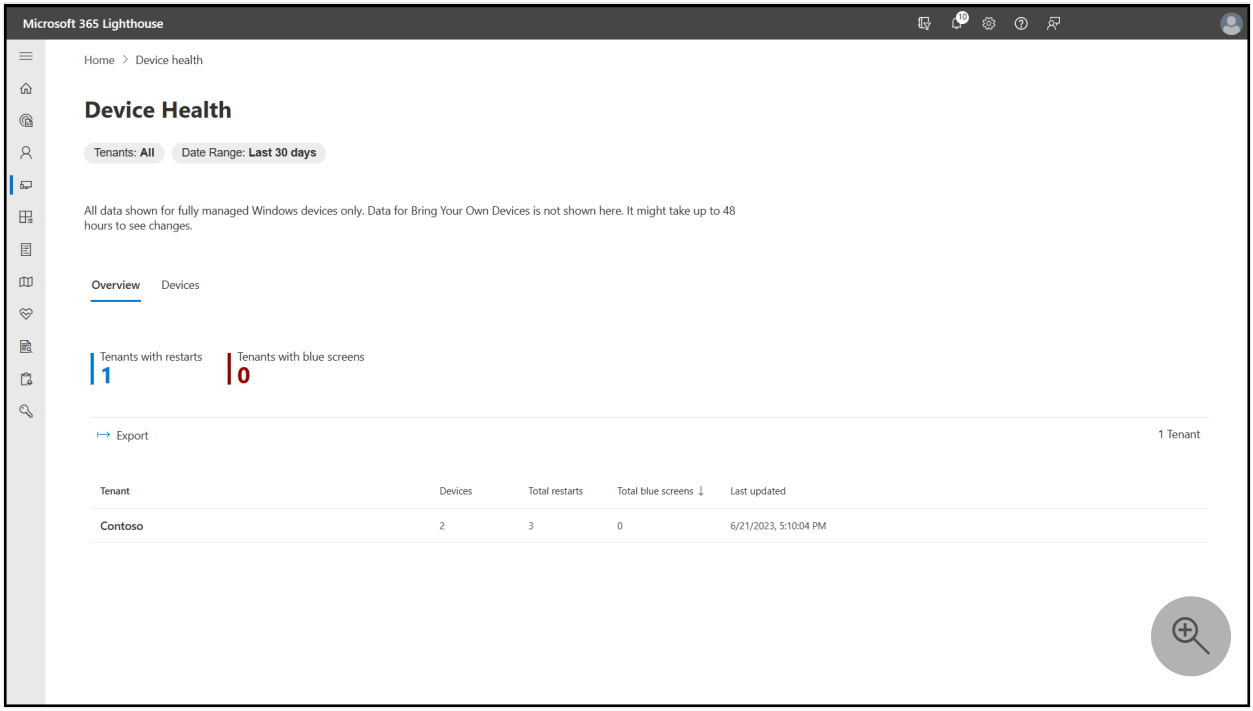
inscripción de dispositivos, compruebe que la **directiva de supervisión del estado** del dispositivo es compatible. Si no es compatible, implemente la directiva.

Pestaña da Información general

La pestaña Información general proporciona una vista multiinquilino del estado del dispositivo, incluido el número total de reinicios y pantallas azules. Seleccione un inquilino de la lista para ver los detalles específicos del dispositivo.

La pestaña Información general también incluye las siguientes opciones:

- **Filtro de inquilinos:** Filtre por inquilino o etiqueta.
- **Filtro de fecha:** Filtre por intervalo de fechas.
- **Exportar**: seleccione esta opción para exportar los datos del dispositivo a un archivo de valores separados por comas (.csv) de Excel.



Pestaña Dispositivos

La pestaña Dispositivo proporciona información sobre el estado del dispositivo para todos los dispositivos Windows administrados, incluidos,

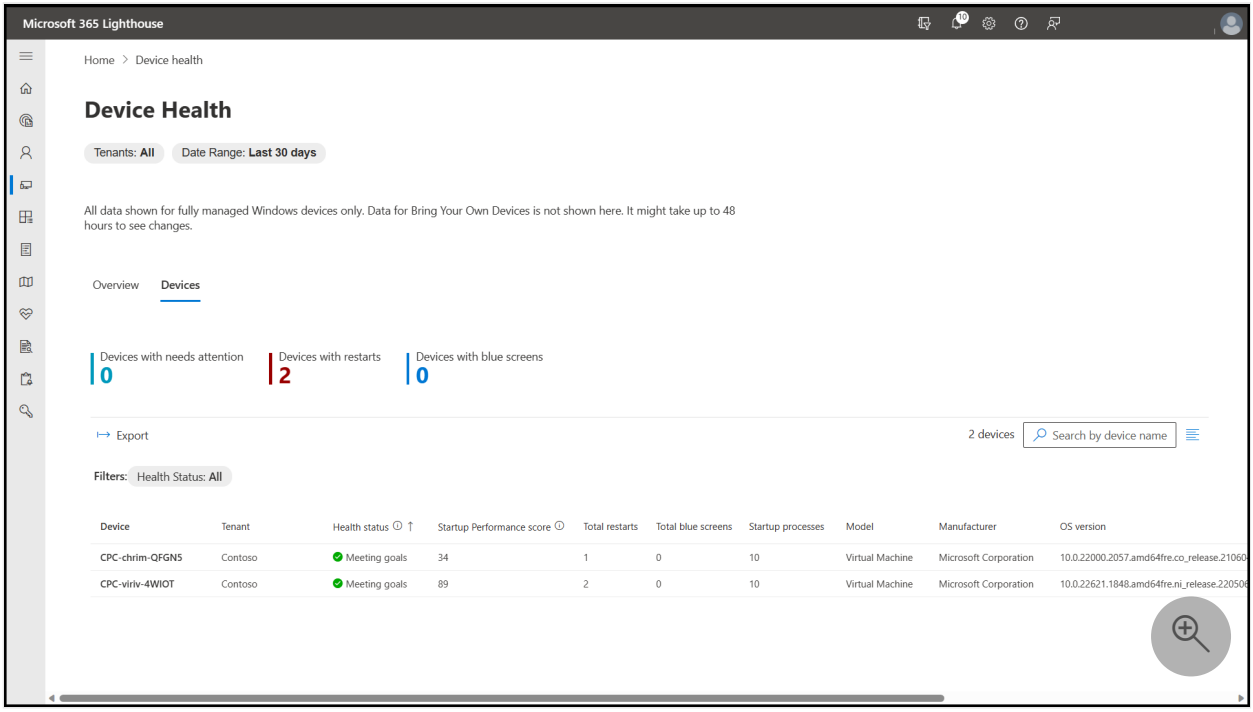
- Estado de mantenimiento (Necesita atención, Objetivos de reunión, Datos insuficientes)

- Puntuación de rendimiento de inicio: para obtener más información, consulte Puntuaciones, líneas base e información en Análisis de puntos de conexión.
- Reinicios totales
- Total de pantallas azules
- Procesos de inicio
- Modelo de hardware, fabricante, versión del sistema operativo y tipo de disco

Seleccione un dispositivo de la lista para obtener información más detallada del dispositivo, incluida una lista completa de procesos de inicio en ese dispositivo. Se proporciona un acceso directo para ver el dispositivo en Microsoft Endpoint Manager, donde puede ver más información y recomendaciones.

La pestaña Dispositivos también incluye las siguientes opciones:

- **Filtro de inquilinos:** Filtre por inquilino o etiqueta.
- **Filtro de fecha:** Filtre por intervalo de fechas.
- **Exportar**: seleccione esta opción para exportar los datos del dispositivo a un archivo de valores separados por comas (.csv) de Excel.
- **Búsqueda**: escriba palabras clave para localizar rápidamente un dispositivo específico en la lista.
- **Elija Columnas**: seleccione las columnas que se van a mostrar.



Contenido relacionado

¿Qué es el análisis de punto de conexión? (artículo)
Puntuaciones, líneas base e información en Análisis de puntos de conexión (artículo)
Información general de la página Aplicaciones de Microsoft 365 Lighthouse (artículo)

Información general de la página Cumplimiento de dispositivos en Microsoft 365 Lighthouse

Artículo • 27/10/2023

Microsoft 365 Lighthouse permite ver información e información relacionada con el cumplimiento de dispositivos de Intune para todos los inquilinos del cliente seleccionando **Dispositivos**>**Cumplimiento** de dispositivos en el panel de navegación izquierdo para abrir la página Cumplimiento de dispositivos. En esta página, puede obtener información general sobre el estado de cumplimiento entre inquilinos, ver una lista de dispositivos para cada inquilino y obtener informes de estado sobre las directivas de cumplimiento y la configuración.

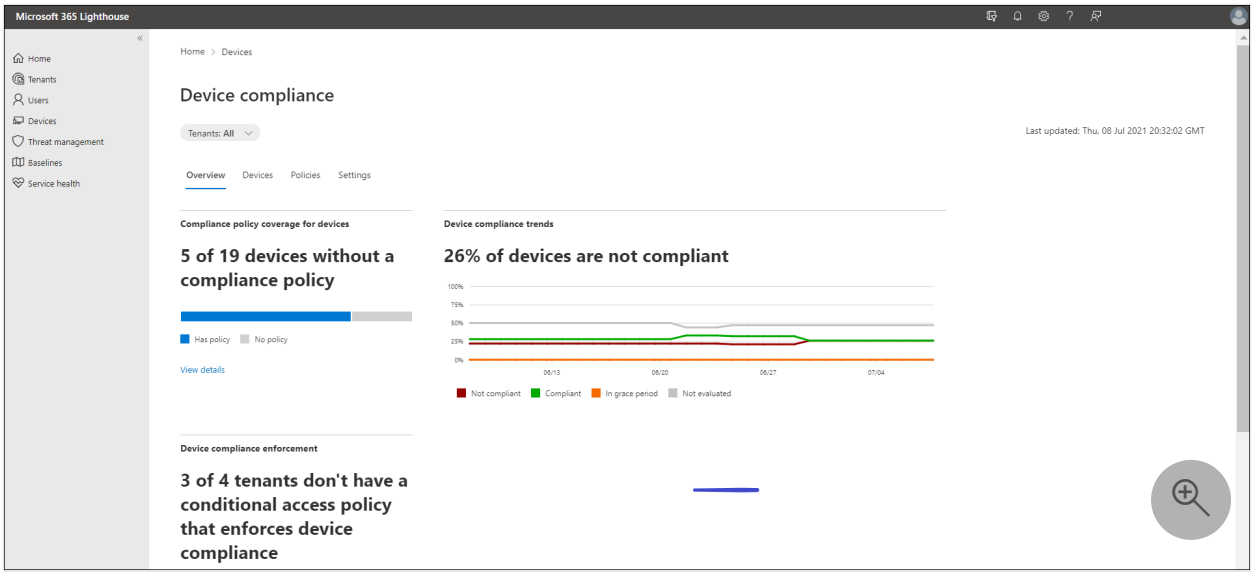
> **Nota**
>
> En esta página se proporciona el número de inquilinos para los que los datos no están disponibles porque no tienen las licencias necesarias.

Pestaña da Información general

En la pestaña Información general, puede ver el estado de cumplimiento de los dispositivos entre los inquilinos, ver las tendencias de cumplimiento de dispositivos mensuales y realizar un seguimiento de si los dispositivos tienen asignadas directivas de cumplimiento. También puede ver cuántos inquilinos no tienen ningún requisito de cumplimiento de dispositivos aplicado mediante directivas de acceso condicional. Puede seleccionar **Ver más** para ver más detalles.

Para obtener información detallada sobre el cumplimiento de dispositivos para un inquilino de cliente determinado, seleccione un valor en cualquiera de las columnas de estado de ese inquilino. Se abrirá la pestaña Dispositivos para que pueda ver los detalles de cumplimiento del dispositivo para el inquilino seleccionado.

Para exportar datos de cumplimiento de dispositivos a un archivo de valores separados por comas (.csv) de Excel, seleccione **Exportar**.



Pestaña Dispositivos

En la pestaña Dispositivos, la barra de anotaciones de recuento de colores muestra el número total de dispositivos en todos los inquilinos del cliente que tienen los siguientes estados de cumplimiento: Compliant, Not compliant, In grace period y Not evaluated. Para obtener más información sobre los diferentes estados de cumplimiento, consulte Supervisión de directivas de cumplimiento de dispositivos de Intune.

Para ver qué inquilinos tienen dispositivos con un estado de cumplimiento específico, seleccione ese estado en la barra count-annotation para filtrar la lista. Para ver los estados de cumplimiento de dispositivos para uno o más inquilinos de clientes específicos, use el menú desplegable **Inquilinos** para filtrar la lista.

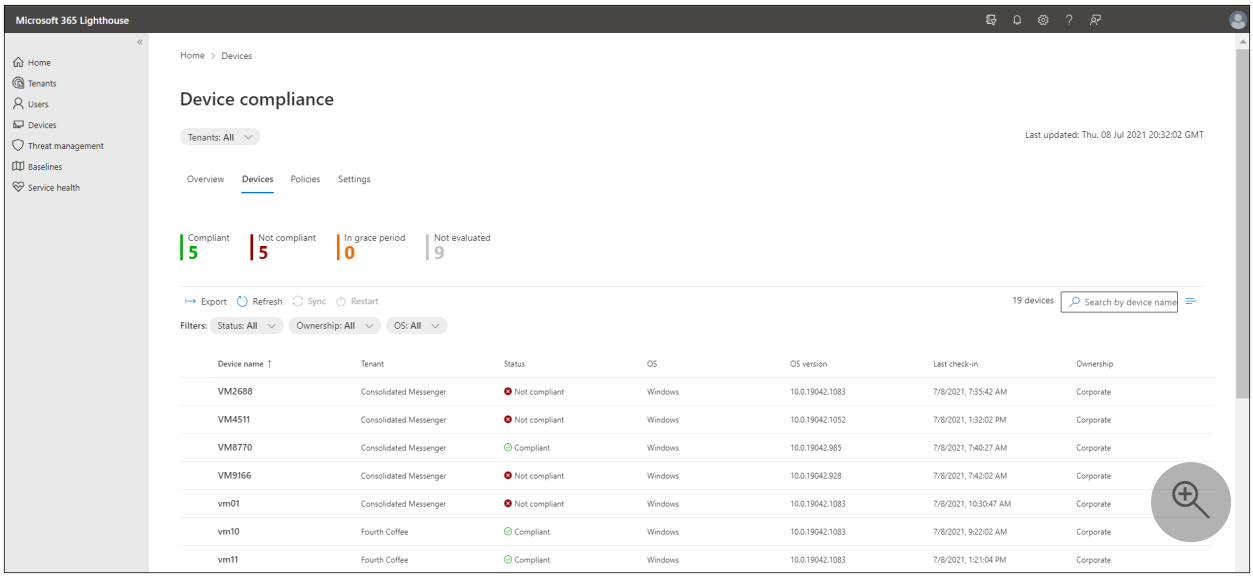
Seleccione cualquier nombre de dispositivo en la lista para ver más detalles sobre el estado de cumplimiento actual del dispositivo. Puede sincronizar o reiniciar el dispositivo, o bien seleccionar **Ver dispositivo en Microsoft Endpoint Manager** si necesita solucionar problemas o realizar otras acciones.

> ⓘ **Nota**
>
> Al reiniciar un dispositivo, el propietario del dispositivo no recibe una notificación automática y puede perder el trabajo no guardado. Por este motivo, es posible que quiera notificar al propietario del dispositivo antes de reiniciar un dispositivo.

La pestaña Dispositivos también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar los datos de cumplimiento de dispositivos a un archivo de valores separados por comas (.csv) de Excel.

- **Actualizar:** Seleccione esta opción para recuperar los datos de cumplimiento de dispositivos más actuales.
- **Sincronizar:** Seleccione uno o varios dispositivos de la lista que tengan el estado No compatible, En período de gracia o No evaluado y, a continuación, seleccione esta opción para forzar a esos dispositivos a protegerse con Intune y recibir inmediatamente las directivas que se les hayan asignado.
- **Reiniciar:** Seleccione uno o varios dispositivos de la lista que tengan el estado No compatible, En período de gracia o No evaluado y, a continuación, seleccione esta opción para reiniciar esos dispositivos.
- **Búsqueda:** Escriba palabras clave para localizar rápidamente un dispositivo específico en la lista.



Pestaña Directivas

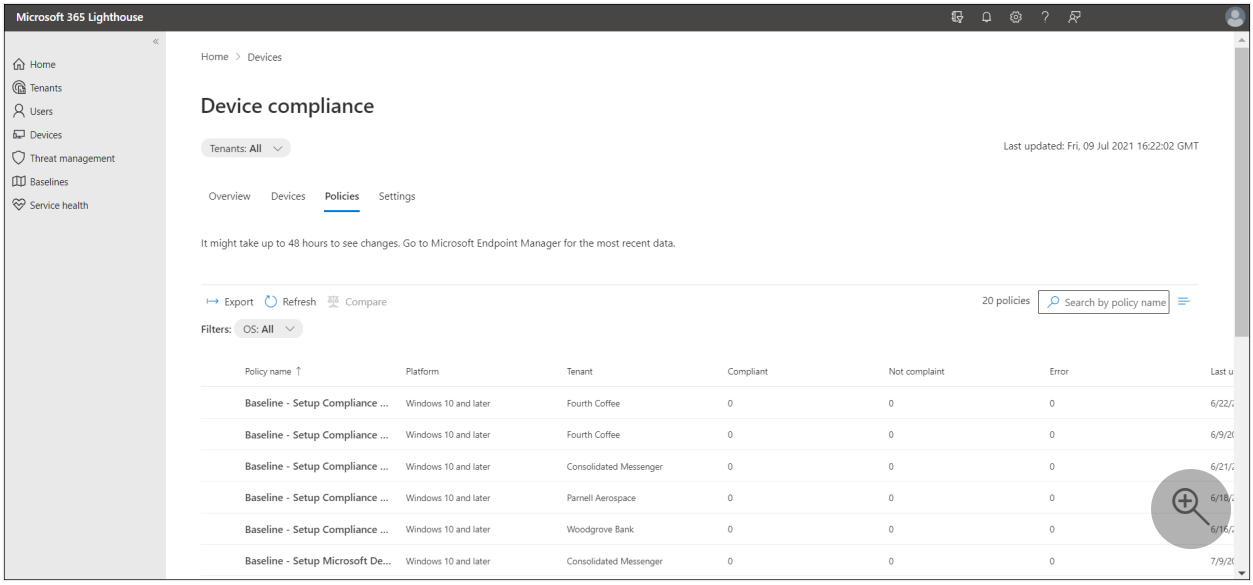
En la pestaña Directivas, puede ver las directivas de cumplimiento de dispositivos entre los inquilinos y comparar dos o tres directivas del mismo tipo de plataforma mediante la opción **Comparar** .

Para ver las directivas de los dispositivos en una plataforma específica, use el menú desplegable del **sistema** operativo para filtrar la lista. Para ver las directivas de uno o más inquilinos de clientes específicos, use el menú desplegable **Inquilinos** para filtrar la lista.

Seleccione cualquier nombre de directiva de la lista para ver más detalles sobre esa directiva. Si necesita realizar acciones o ver información adicional, seleccione **Ver esta directiva en Microsoft Endpoint Manager**.

La pestaña Directivas también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar los datos de la directiva de cumplimiento de dispositivos a un archivo de valores separados por comas (.csv) de Excel.
- **Actualizar:** Seleccione esta opción para recuperar los datos más actuales de la directiva de cumplimiento de dispositivos.
- **Búsqueda:** Escriba palabras clave para localizar rápidamente una directiva de cumplimiento de dispositivos específica en la lista.



Pestaña Configuración

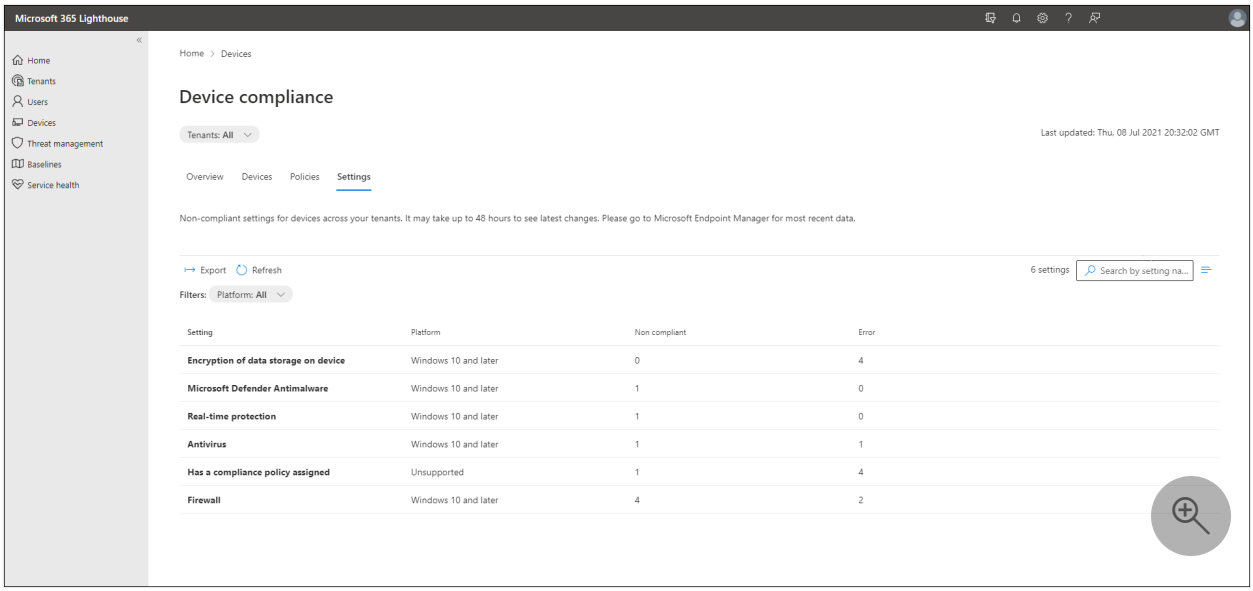
La pestaña Configuración proporciona un informe agregado de la configuración no compatible entre dispositivos de inquilino.

Para ver la configuración no compatible para dispositivos en una plataforma específica, use el menú desplegable **Plataforma** para filtrar la lista. Para ver la configuración no compatible para uno o más inquilinos de clientes específicos, use el menú desplegable **Inquilinos** para filtrar la lista.

Seleccione cualquier nombre de configuración no compatible en la lista para abrir un panel donde pueda ver una lista de inquilinos que tienen dispositivos con esa configuración específica no compatible. Desde aquí, puede explorar en profundidad aún más si selecciona cualquier inquilino de la lista para ver información sobre los dispositivos dentro de ese inquilino que tienen la configuración específica no compatible. También puede sincronizar o reiniciar el dispositivo, o bien seleccionar **Ver dispositivo en Microsoft Endpoint Manager** si necesita solucionar problemas o realizar otras acciones.

La pestaña Configuración también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar datos de configuración no compatibles a un archivo de valores separados por comas (.csv) de Excel.
- **Actualizar:** Seleccione esta opción para recuperar los datos de configuración no compatibles más actuales.
- **Búsqueda:** Escriba palabras clave para localizar rápidamente una configuración específica no compatible en la lista.



Contenido relacionado

Comparar la configuración de la directiva de cumplimiento de dispositivos en Microsoft 365 Lighthouse (artículo)
Información general de la página Estado del dispositivo en Microsoft 365 Lighthouse (artículo)
Información general de la página Windows 365 (PC en la nube) en Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)

Comparar la configuración de la directiva de cumplimiento de dispositivos en Microsoft 365 Lighthouse

Artículo • 03/10/2024

Microsoft 365 Lighthouse permite ver las directivas de cumplimiento entre los inquilinos en una sola vista. Puede impulsar la seguridad y la estandarización entre los inquilinos mediante la comparación de directivas. Puede filtrar las vistas para ver la configuración que se ha configurado (frente a la configuración que no se ha configurado), la configuración que difiere en sus configuraciones o la configuración que coincide. También puede buscar configuraciones específicas para ver cómo se comparan entre directivas.

Antes de empezar

Asegúrese de que los dispositivos tengan una licencia de Microsoft Intune y que estén inscritos en Microsoft Intune.

Comparación de la configuración de directiva

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Dispositivos**>**cumplimiento de dispositivos**.
2. Seleccione la pestaña **Directivas**.
3. En el filtro del **sistema operativo** , seleccione un sistema operativo o una plataforma.

   > **Nota**
   >
   > Solo puede comparar directivas con el mismo sistema operativo o plataforma.

4. En la lista filtrada, seleccione hasta tres directivas que quiera comparar.
5. Seleccione **Comparar**.

Puede filtrar los resultados para ver **Configuración diferente**, **Configuración que coincide** o **Configuración configurada**.

Configuración de la directiva

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Dispositivos**>**cumplimiento de dispositivos**.
2. Seleccione la pestaña **Directivas**.
3. En la lista de directivas, seleccione la directiva que desea configurar.
4. En el panel de detalles de la directiva, seleccione **Ver esta directiva en Microsoft Intune centro de administración**.
5. En el centro de administración de Microsoft Intune, configure las opciones de directiva según sea necesario.

Pasos siguientes

A medida que realice ajustes de directiva, asegúrese de evaluar los cambios con respecto a la configuración de línea base actual. Para obtener más información, consulte Información general sobre el uso de líneas base para implementar configuraciones de inquilino estándar.

Contenido relacionado

¿Qué es la inscripción de dispositivos en Intune? (artículo)
Usar directivas de cumplimiento para establecer reglas para los dispositivos que administra con Intune (artículo)
Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Información general de la página Windows 365 (PC en la nube) en Microsoft 365 Lighthouse

Artículo • 04/06/2024

Windows 365 es un servicio basado en la nube que permite a los administradores de Microsoft Intune aprovisionar y administrar equipos en la nube para sus usuarios que tienen una licencia de Windows 365. Windows 365 está totalmente integrado con Intune para la administración de dispositivos y con la administración del proveedor de servicios administrados (MSP) de Microsoft 365 Lighthouse para pc en la nube en todos sus inquilinos de clientes.

Para obtener más información sobre Windows 365, consulta ¿Qué es Windows 365? Para obtener una lista de los requisitos de Windows 365, consulta Requisitos para Windows 365.

> **Importante**
>
> Debe ir al Centro de **administración de Microsoft Intune** para aprovisionar equipos en la nube para cada inquilino de cliente antes de poder administrarlos en Lighthouse. No se puede aprovisionar desde Lighthouse.

Una vez que haya aprovisionado equipos en la nube para el inquilino del cliente, la tarjeta de Windows 365 en la página principal de Microsoft 365 Lighthouse proporciona una breve alerta sobre los equipos en la nube que necesitan acción, como el número de equipos en la nube que no se pudieron aprovisionar y los errores de conexión de red de Azure. Para obtener un estado detallado, seleccione el botón de la tarjeta de Windows 365 (o seleccione **Dispositivos**>**Windows 365** en el panel de navegación izquierdo de Lighthouse) para abrir la página de Windows 365. En esta página, puede obtener información general sobre el estado de los equipos en la nube asignados a los inquilinos del cliente, ver una lista de todos los equipos en la nube que administra y los inquilinos a los que están asignados y ver las conexiones de red de Azure entre los inquilinos del cliente y el identificador de Microsoft Entra y su estado.

Pestaña da Información general

En la pestaña Información general, la barra de anotaciones de recuento de colores muestra el número total de equipos en la nube o conexiones de red de Azure en todos

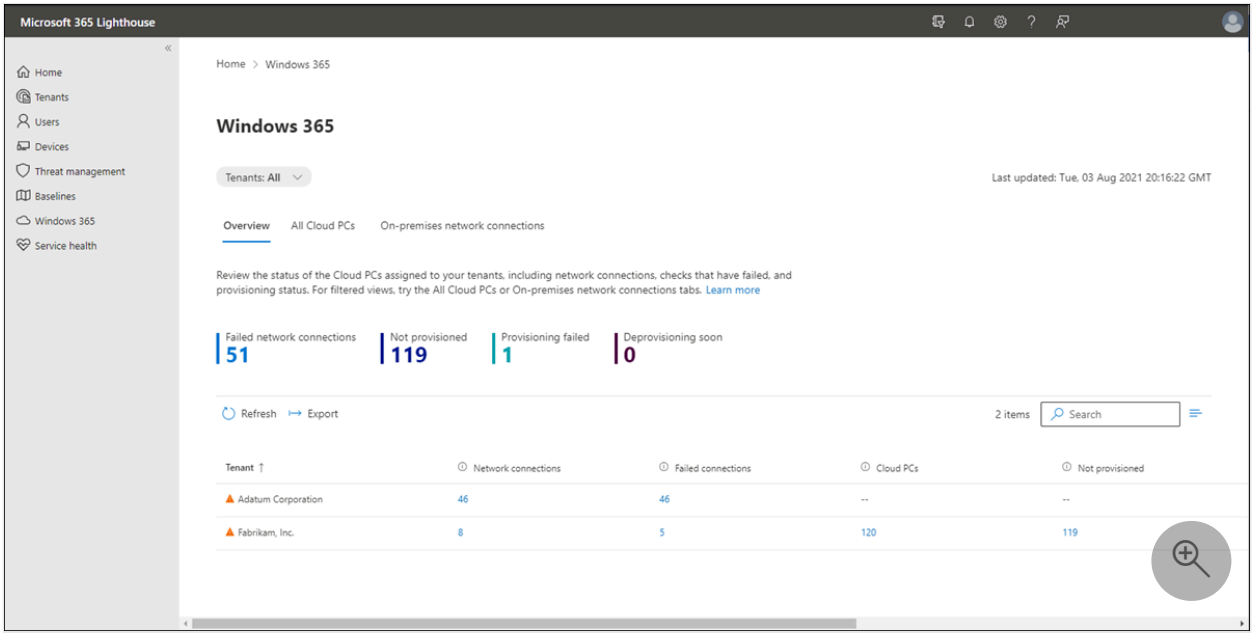
los inquilinos de cliente que tienen los siguientes estados: Conexiones de red con errores, No aprovisionadas, Error de aprovisionamiento y Desaprovisionamiento pronto.

Puede ver un desglose de los estados del equipo en la nube para cada inquilino de cliente en la lista debajo de la barra de anotación de recuento. Para ver qué inquilinos tienen equipos en la nube con un estado específico, seleccione ese estado en la barra count-annotation para filtrar la lista. Para ver los estados del equipo en la nube para uno o más inquilinos de clientes específicos, use el menú desplegable **Inquilinos** para filtrar la lista.

Para obtener información detallada sobre el estado de un inquilino de cliente determinado, seleccione un valor en cualquiera de las columnas de estado de ese inquilino. En función de la columna en la que se encuentra el valor, se abrirá la pestaña **Conexiones de red de Azure** o **Todos los equipos en la nube** y se mostrará más información.

La pestaña Información general también incluye las siguientes opciones:

- **Actualizar:** Seleccione esta opción para recuperar los datos de PC en la nube más actuales.
- **Exportar:** Seleccione esta opción para exportar los datos de Cloud PC a un archivo de valores separados por comas (.csv) de Excel.
- **Búsqueda:** Escriba palabras clave para localizar rápidamente un equipo en la nube específico en la lista.



Pestaña Todos los equipos en la nube

En la pestaña Todos los equipos en la nube, la barra de anotaciones de recuento de colores muestra el número total de equipos en la nube en todos los inquilinos de cliente que tienen los siguientes estados: Aprovisionado, No aprovisionado, Error de aprovisionamiento y Desaprovisionamiento pronto.

Puede ver todos los equipos en la nube y su estado de aprovisionamiento en la lista debajo de la barra count-annotation. Se proporciona la siguiente información:

- **Nombre del equipo en la nube:** Nombre asignado al equipo en la nube.
- **Usuario:** Usuario para el que se ha aprovisionado o intentado aprovisionar un equipo en la nube.
- **Nombre del dispositivo:** Nombre del dispositivo de Intune: un identificador único para un equipo en la nube.
- **Inquilino:** Inquilino del cliente en el que se aprovisionó un equipo en la nube.
- **Estado:** Estado de aprovisionamiento del equipo en la nube.
- **Tipo de licencia:** Empresa o Empresa.
- **Especificaciones:** Configuración de hardware de PC en la nube.

Para ver qué inquilinos tienen equipos en la nube con un estado de aprovisionamiento específico, seleccione ese estado en la barra count-annotation para filtrar la lista. Para ver los estados de aprovisionamiento de equipos en la nube para uno o más inquilinos de clientes específicos, use el menú desplegable **Inquilinos** para filtrar la lista.

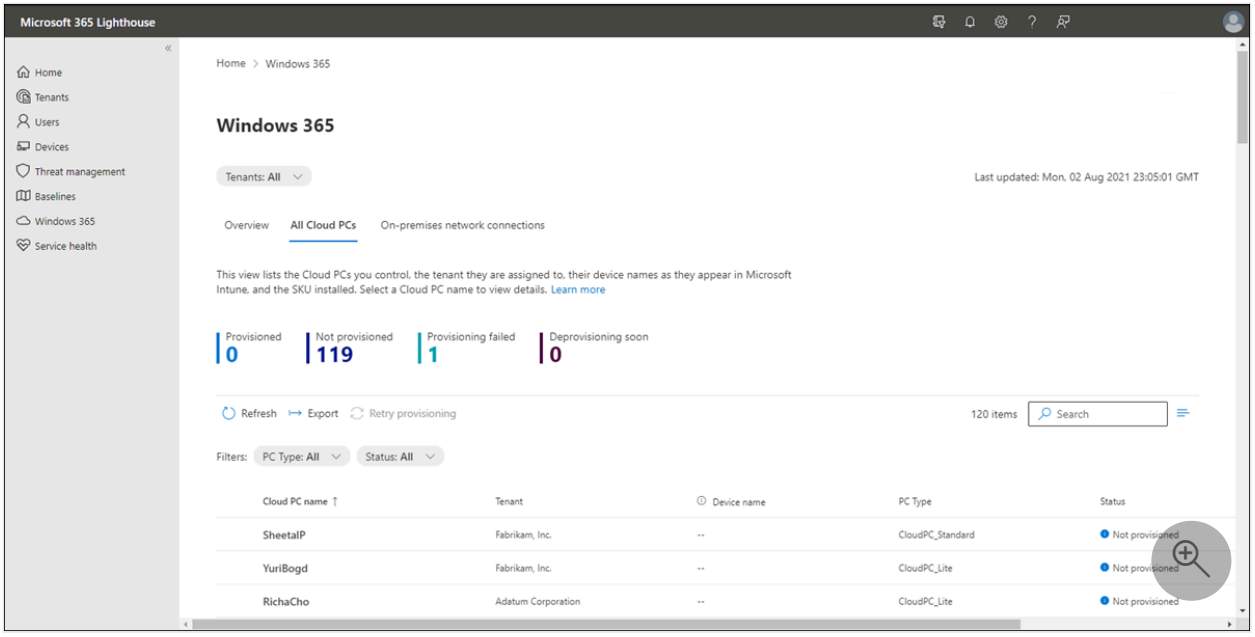
Seleccione cualquier equipo en la nube en la lista para ver más detalles y ejecutar acciones de administración como:

- **Reiniciar:** Seleccione esta opción para reiniciar el dispositivo.
- **Reprovision:** Seleccione esta opción para restablecer el dispositivo. También puede ver la directiva de aprovisionamiento en el vínculo de Microsoft Intune.
- **Renombrar:** Seleccione esta opción para cambiar el nombre del dispositivo asignado a un usuario.
- **Cambiar tipo de cuenta:** Seleccione el tipo de cuenta para el usuario: Usuario estándar (recomendado) o Administrador local.

La pestaña Todos los equipos en la nube también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar los datos de Cloud PC a un archivo de valores separados por comas (.csv) de Excel.
- **Actualizar:** Seleccione esta opción para recuperar los datos de PC en la nube más actuales.
- **Búsqueda:** Escriba palabras clave para localizar rápidamente un equipo en la nube específico en la lista.

Para ver una lista completa de los estados de aprovisionamiento de PC en la nube y lo que significan, consulte Información general sobre la administración de dispositivos para pc en la nube en la biblioteca de documentación de Windows 365.



Pestaña Conexiones de red de Azure

En la pestaña Conexiones de red de Azure, la barra de anotaciones de recuento de colores muestra el número total de conexiones de red de Azure en todos los inquilinos de cliente que tienen equipos con Windows 365 Enterprise Cloud y que pueden tener los siguientes estados: Conexiones correctas y Conexiones con errores.

En la lista debajo de la barra count-annotation, puede ver todas las conexiones de red de Azure y su estado de conexión.

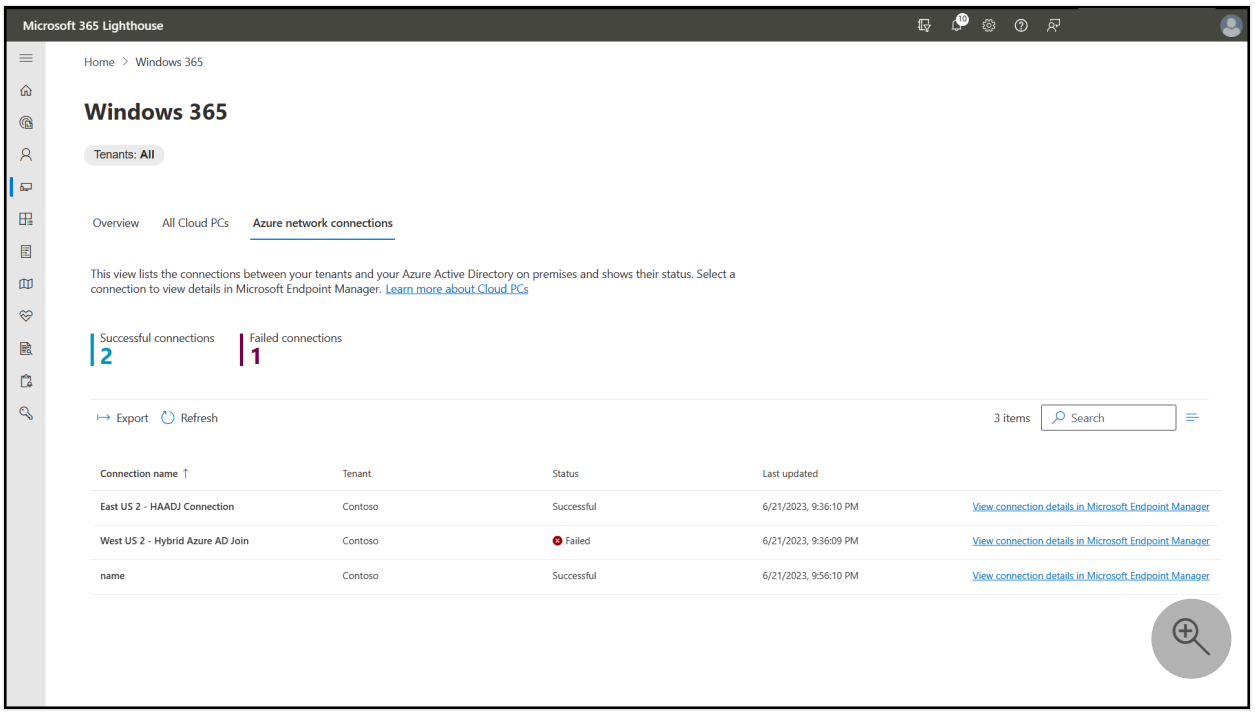
Para ver las conexiones con un estado de aprovisionamiento específico, seleccione ese estado en la barra count-annotation para filtrar la lista. Para ver los estados de conexión de uno o más inquilinos de clientes específicos, use el menú desplegable **Inquilinos** para filtrar la lista.

Si necesita realizar acciones o solucionar problemas de una conexión en la lista, seleccione **Ver detalles de conexión en Microsoft Endpoint Manager**.

La pestaña Conexiones de red de Azure también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar los datos de conexión a un archivo de valores separados por comas (.csv) de Excel.
- **Actualizar:** Seleccione esta opción para recuperar los datos de conexión más actuales.

- **Búsqueda:** Escriba palabras clave para localizar rápidamente una conexión específica.



Contenido relacionado

¿Qué es Windows 365? (artículo)
Información general sobre la administración de dispositivos windows 365 para pc en la nube (artículo)
Preguntas más frecuentes sobre Lighthouse de Microsoft 365 (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Reprovisione un PC en la nube Windows 365 en Microsoft 365 Lighthouse

Artículo • 20/01/2025

Microsoft 365 Lighthouse admite el reaprovisionamiento de equipos en la nube que tienen una directiva de aprovisionamiento. Es posible que tenga que volver a aprovisionar un dispositivo para un nuevo usuario o si el dispositivo no funciona correctamente. Cuando se desencadena un reaprovisionamiento, el equipo en la nube se elimina y se vuelve a crear como un nuevo equipo en la nube. Se eliminan todos los datos de usuario, las aplicaciones y las personalizaciones.

Antes de empezar

Debe tener el rol Administrador de PC en la nube en Microsoft Intune para volver a aprovisionar un PC en la nube Windows 365 en Lighthouse.

Reprovisione un PC en la nube Windows 365

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Dispositivos**>**Windows 365**.
2. Seleccione la pestaña **Todos los equipos en la nube** .
3. En la lista desplegable **Filtros** , seleccione Tipo de licencia.
4. En la lista filtrada, seleccione un dispositivo.
5. En el panel de detalles del dispositivo, seleccione **Reprovisionar**.
6. En el cuadro de diálogo de confirmación, seleccione **Sí, reprovisione este equipo** en la nube y, a continuación, seleccione **Reprovisionar**.

> **Nota**
>
> El usuario actual del equipo en la nube se ha iniciado sesión inmediatamente y se quitan todos los datos de usuario.

Comprobación del estado de la acción del dispositivo

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Dispositivos**>**Windows 365**.
2. Seleccione la pestaña **Todos los equipos en la nube** .
3. En la lista de dispositivos, seleccione un dispositivo.
4. En el panel de detalles del dispositivo, seleccione la pestaña **Estado de la acción del dispositivo** .

La pestaña muestra el estado de la acción más reciente en cola para el dispositivo seleccionado, incluidos el tipo de acción, el estado y la marca de tiempo.

Contenido relacionado

Información general sobre el aprovisionamiento (artículo)
Editar directivas de aprovisionamiento (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Cambiar un tipo de cuenta de pc en la nube de Windows 365 Business en Microsoft 365 Lighthouse

Artículo • 20/01/2025

Los técnicos del proveedor de servicios administrados (MSP) pueden establecer el tipo de cuenta de un equipo de Business Cloud o realizar cambios en un tipo de cuenta existente. Están disponibles los siguientes tipos de cuenta:

- **Standard usuario (recomendado):** Standard cuentas de usuario tienen permiso para instalar software solo desde Microsoft Store.
- **Administrador local** : las cuentas de administrador local tienen permiso para instalar cualquier software y realizar cambios en cualquier parte del sistema operativo. Seleccione este tipo de cuenta solo cuando sea necesario, ya que el malware puede usar permisos de administrador para infectar o dañar archivos.

> ⓘ **Nota**
>
> Puede establecer o cambiar el tipo de cuenta solo para equipos en la nube con una licencia de empresa. No se puede cambiar el tipo de cuenta de los equipos en la nube con una licencia enterprise.

Antes de empezar

Debe tener el rol Administrador de PC en la nube (recomendado) o Administrador de Windows 365 en Microsoft Intune para establecer o cambiar un tipo de cuenta de pc en la nube de Windows 365 Business en Lighthouse.

> ⊗ **Precaución**
>
> Para ayudar a proteger su organización, Microsoft recomienda usar roles con el nivel mínimo de permisos necesarios para realizar un trabajo.

Establecimiento o cambio de un tipo de cuenta de pc en la nube de Windows 365 Business

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Dispositivos**>**Windows 365**.
2. Seleccione la pestaña **Todos los equipos en la nube** .
3. Use la barra de anotaciones de recuento de colores para explorar en profundidad los equipos en la nube que tienen un estado **Aprovisionado** .
4. En el menú desplegable **Filtros** , seleccione el tipo de licencia **Business** para ver una lista de todos los equipos en la nube con una licencia empresarial dentro de los inquilinos del cliente.
5. En la lista de equipos en la nube, seleccione el equipo en la nube para el que desea cambiar el tipo de cuenta.
6. En el panel de detalles del equipo en la nube, seleccione **Cambiar tipo de cuenta**.
7. En el panel **Cambiar tipo de cuenta de PC** en la nube, seleccione el tipo de cuenta para el equipo en la nube y, a continuación, seleccione **Guardar**.

Pasos siguientes

Una vez aplicada la actualización, el usuario asignado del equipo en la nube tendrá que volver a iniciar sesión en el equipo en la nube o reiniciar el dispositivo. Los nuevos cambios pueden tardar varios minutos en aparecer en Microsoft 365 Lighthouse. El administrador de PC en la nube también puede reiniciar de forma remota el equipo en la nube, pero el usuario puede perder los datos no guardados.

Contenido relacionado

Control de acceso basado en rol de PC en la nube (artículo)
Información general de la página Windows 365 (PC en la nube) en Microsoft 365 Lighthouse (artículo)
Reprovisionar un PC en la nube Windows 365 en Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Visualización de una conexión de red con errores en un equipo en la nube empresarial en Microsoft 365 Lighthouse

Artículo • 20/01/2025

Microsoft 365 Lighthouse proporciona el estado de conexión entre los inquilinos del cliente y Microsoft Entra ID. Cuando un equipo en la nube tiene una conexión de red errónea, puede ver información detallada en el centro de administración de Microsoft Intune.

Antes de empezar

Debe tener el rol Administrador de PC en la nube o Lector de PC en la nube en Microsoft Intune para ver los problemas de conexión.

Visualización de una conexión de red con errores

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Dispositivos**>**Windows 365**.
2. Seleccione la pestaña **Conexiones de red de Azure** .
3. En la barra de anotaciones de recuento de colores, seleccione **Conexiones con errores**.
4. En la lista filtrada, seleccione **Ver detalles de conexión en Microsoft Intune centro de administración** junto a la conexión que desea investigar.
5. En el centro de administración de Microsoft Intune, seleccione **Ver detalles** para obtener más información sobre el error.

Pasos siguientes

Para solucionar problemas de conexión, consulte Solución de problemas de conexión de red local.

Contenido relacionado

Control de acceso basado en rol de PC en la nube (artículo)
Unión al dominio de Active Directory (artículo)
Microsoft Entra device Sync (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Información general de la página Administración de amenazas en Microsoft 365 Lighthouse

Artículo • 28/10/2023

Se aplica a:

- Windows

Microsoft Defender Antivirus protege a los inquilinos, usuarios y dispositivos frente a amenazas de software, incluidos virus, malware y spyware. Es una protección sólida y continua que está integrada en Windows.

Para acceder a la página Administración de amenazas de Microsoft 365 Lighthouse, seleccione**Administración de amenazas** de **dispositivos**> en el panel de navegación izquierdo para ver la posición de seguridad de los inquilinos del cliente frente a amenazas. Verá inquilinos, usuarios y dispositivos que requieren su atención y recomendaciones que le ayudarán a reducir el riesgo.

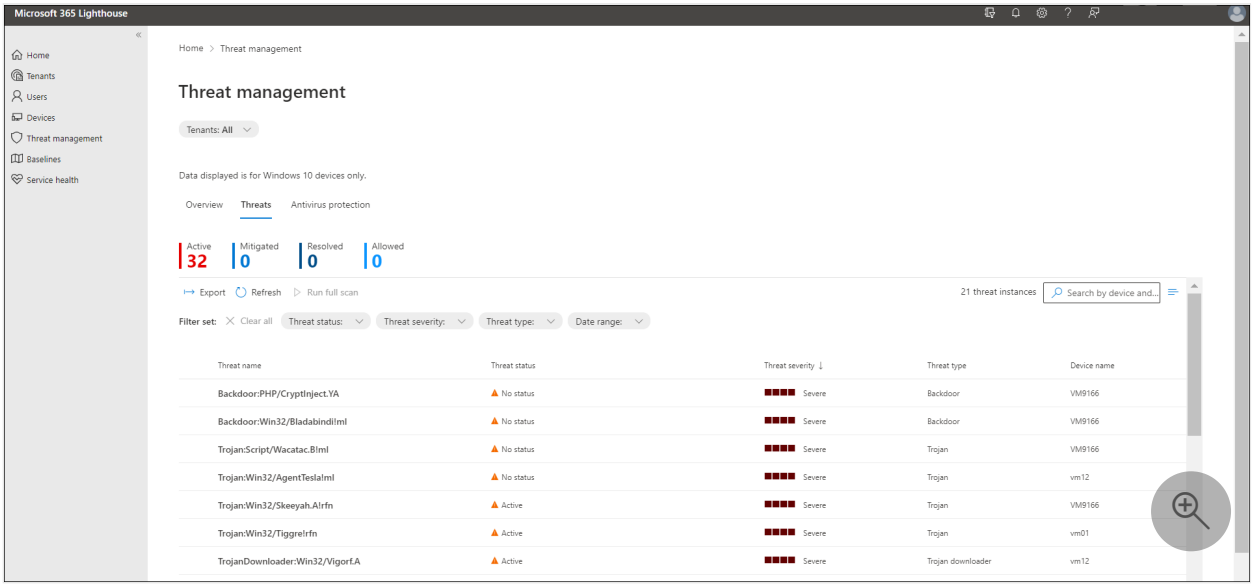
> ⓘ **Nota**
>
> En esta página se proporciona el número de inquilinos para los que los datos no están disponibles porque no tienen las licencias necesarias.

Pestaña da Información general

En la pestaña Información general de la página Administración de amenazas, puede supervisar el estado del antivirus en todos los inquilinos para identificar las áreas que necesitan atención.

Pestaña Amenazas

En la pestaña Amenazas de la página Administración de amenazas, puede ver las amenazas activas, mitigadas, resueltas y permitidas en todos los inquilinos. También puede corregir varias amenazas al mismo tiempo en todos los inquilinos mediante el filtrado y la exploración en profundidad de cada amenaza para saber qué dispositivos, usuarios o inquilinos se ven afectados.



Puede filtrar las amenazas por:

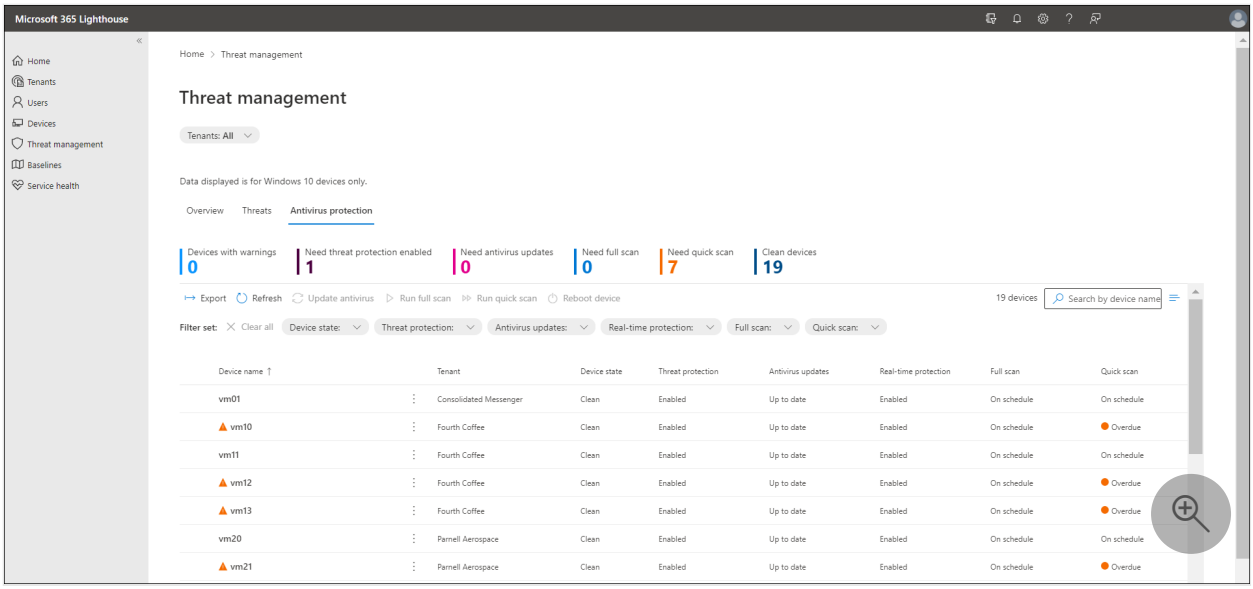
- Estado de la amenaza
- Gravedad de la amenaza
- Tipo de amenaza
- Intervalo de fechas

En la tabla siguiente se enumeran los distintos estados de amenaza y su definición:

Estado de la amenaza	Definición
Activo	La amenaza está activa en el dispositivo.
Sin estado	El estado de la amenaza no está disponible. Ejecute un examen completo en el dispositivo para que Microsoft Defender Antivirus vuelva a detectar la amenaza.
Error en la acción	El dispositivo no está en riesgo. Se ha producido un error en una acción, pero se ha detenido una amenaza potencial y no está activa en el dispositivo. Ejecute un examen completo en el dispositivo.
Pasos manuales necesarios	La amenaza se ha detenido, pero requiere que se complete un paso manual, como un examen completo o un reinicio del dispositivo.
Examen completo necesario	Se requiere un examen completo del dispositivo.
Reinicio necesario	Se requiere un reinicio del dispositivo.
Corregido con errores no críticos	La amenaza se ha corregido y no se necesitan más acciones.
Cuarentena	La amenaza se ha puesto en cuarentena. No se necesitan más acciones.
Eliminación	La amenaza se ha quitado correctamente del dispositivo. No se necesitan más acciones.
Limpiado	Microsoft Defender Antivirus ha recuperado y desinfectado archivos. No se necesitan más acciones.
Permitido	Un administrador permite que la amenaza permanezca en el dispositivo.

Pestaña Protección antivirus

La pestaña Protección antivirus de la página Administración de amenazas muestra los dispositivos en todos los inquilinos y su estado de protección antivirus Microsoft Defender. Puede evaluar el estado y tomar medidas para uno o varios dispositivos que pueden ser vulnerables. También puede seleccionar un dispositivo para ver más información, como Información general del dispositivo, Amenazas actuales y Estados de acción del dispositivo.



Contenido relacionado

Información general sobre el uso de líneas base de Microsoft 365 Lighthouse para implementar configuraciones de inquilino estándar (artículo)

Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)

Mitigación de amenazas en Microsoft 365 Lighthouse con Microsoft Defender Antivirus

Artículo • 28/09/2024

Microsoft 365 Lighthouse permite investigar y mitigar las amenazas en todos los inquilinos. También puede iniciar exámenes antivirus en dispositivos, asegurarse de que los dispositivos obtienen las actualizaciones más recientes de Microsoft Defender Antivirus y revisar las acciones pendientes después de los exámenes antivirus. Lighthouse solo admite dispositivos que ejecutan Windows 10 o posterior.

Antes de empezar

- Microsoft 365 Lighthouse solo se implementa en el inquilino del asociado, no en los inquilinos del cliente, sino que se asegura de que usted y los inquilinos del cliente cumplen los requisitos enumerados en los requisitos de Microsoft 365 Lighthouse.
- Los usuarios deben ejecutar Microsoft Defender Antivirus (incluido con Windows). Lighthouse no admite software antivirus que no sea de Microsoft. Para obtener más información, vea Activar Microsoft Defender Antivirus.
- Debe ser administrador global en el inquilino de asociado en el que está iniciando sesión.

Investigación de amenazas activas

Para investigar una amenaza específica:

1. En el panel de navegación izquierdo de Lighthouse, seleccione Administración**de amenazas dedispositivos**>.
2. Seleccione la pestaña **Amenazas** .
3. En la lista de amenazas, seleccione la amenaza que desea investigar.

El panel de detalles de amenazas proporciona la siguiente información:

Expandir tabla

Categoría	Definición
Dispositivo e inquilino	El nombre del dispositivo y el inquilino donde se encontró la amenaza. Seleccione el nombre del dispositivo para ver información adicional.
Estado de la amenaza	Estado de la amenaza.
Tipo de amenaza	Tipo de amenaza.
Gravedad de la amenaza	Gravedad de la amenaza (grave, alta, moderada, baja, desconocida)
Instancias	Número de instancias de esta amenaza presentes en el dispositivo.
Primera vez detectada	La primera vez que se detectó la amenaza en este dispositivo.
Documentación	Vínculo a información adicional sobre la amenaza.
Otros dispositivos de este inquilino con esta amenaza	Una lista de otros dispositivos del mismo inquilino con la misma amenaza activa.
Otros inquilinos con esta amenaza	Una lista de otros inquilinos con la misma amenaza activa.

Para investigar las amenazas en un dispositivo específico:

1. En el panel de navegación izquierdo de Lighthouse, seleccione Administración**de amenazas dedispositivos**>.
2. Seleccione la pestaña **Protección antivirus** .
3. Seleccione un dispositivo de la lista.
4. En el panel de detalles del dispositivo, seleccione la pestaña **Amenazas actuales** .

Lighthouse muestra todas las amenazas que se encuentran en el dispositivo. Para ver los detalles, seleccione la amenaza.

Buscar amenazas en un dispositivo

Un examen rápido busca ubicaciones comunes en las que podría haber malware, como claves del Registro y carpetas de inicio conocidos. Un examen completo busca en todo el dispositivo. En la mayoría de los casos, un examen rápido es suficiente y es la opción recomendada para los exámenes programados.

1. En el panel de navegación izquierdo de Lighthouse, seleccione Administración**de amenazas dedispositivos**>.
2. Seleccione la pestaña **Protección antivirus** .
3. En la lista de dispositivos, seleccione un dispositivo.
4. En el panel de detalles del dispositivo, seleccione **Ejecutar examen completo** o **Ejecutar examen rápido**.

Para examinar varios dispositivos, active la casilla situada junto a cada nombre de dispositivo de la lista y, a continuación, seleccione **Ejecutar examen completo** o **Ejecutar examen rápido**.

Obtención de actualizaciones para Microsoft Defender Antivirus

Para actualizar Microsoft Defender Antivirus en un único dispositivo:

1. En el panel de navegación izquierdo de Lighthouse, seleccione Administración**de amenazas dedispositivos**>.
2. Seleccione la pestaña **Protección antivirus** .
3. En la lista de dispositivos, seleccione un dispositivo.
4. En el panel de detalles del dispositivo, seleccione **Actualizar antivirus**.

Para obtener actualizaciones para varios dispositivos, active la casilla situada junto a cada nombre de dispositivo de la lista y, a continuación, seleccione **Actualizar antivirus**.

Si necesita crear una nueva directiva, seleccione **Actualizar directiva** en el panel de detalles del dispositivo. Lighthouse le redirigirá al centro de administración de Microsoft Intune. Para obtener más información sobre cómo crear una directiva, vea Crear una directiva de cumplimiento en Microsoft Intune.

Comprobación de las acciones antivirus pendientes en un dispositivo

Cuando se aplican acciones consecutivas a un dispositivo, recibirá un mensaje pendiente de acción. Para comprobar qué acciones están pendientes en un dispositivo:

1. En el panel de navegación izquierdo de Lighthouse, seleccione Administración**de amenazas dedispositivos**>.
2. Seleccione la pestaña **Protección antivirus** .
3. En la lista de dispositivos, seleccione un dispositivo.
4. En el panel de detalles del dispositivo, seleccione la pestaña **Estado de la acción del dispositivo** para ver las acciones pendientes.

Reiniciar un dispositivo

Algunas actualizaciones pueden requerir que un dispositivo se reinicie para instalarse correctamente.

1. En el panel de navegación izquierdo de Lighthouse, seleccione Administración**de amenazas dedispositivos**>.
2. Seleccione la pestaña **Protección antivirus** .
3. En la lista de dispositivos, seleccione un dispositivo.
4. En el panel de detalles del dispositivo, seleccione **Reiniciar dispositivo**.

Para reiniciar varios dispositivos, active la casilla situada junto a cada nombre de dispositivo de la lista y, a continuación, seleccione **Reiniciar dispositivo**.

Contenido relacionado

Requisitos para Microsoft 365 Lighthouse (artículo)
Información general de la página Administración de amenazas en Microsoft 365 Lighthouse (artículo)
Creación de una directiva de cumplimiento en Microsoft Intune (artículo)
Habilitación y configuración de Microsoft Defender protección always-on del Antivirus (artículo)
Inteligencia de seguridad de Microsoft (página web)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Información general de la página Seguridad del dispositivo en Microsoft 365 Lighthouse

Artículo • 04/06/2024

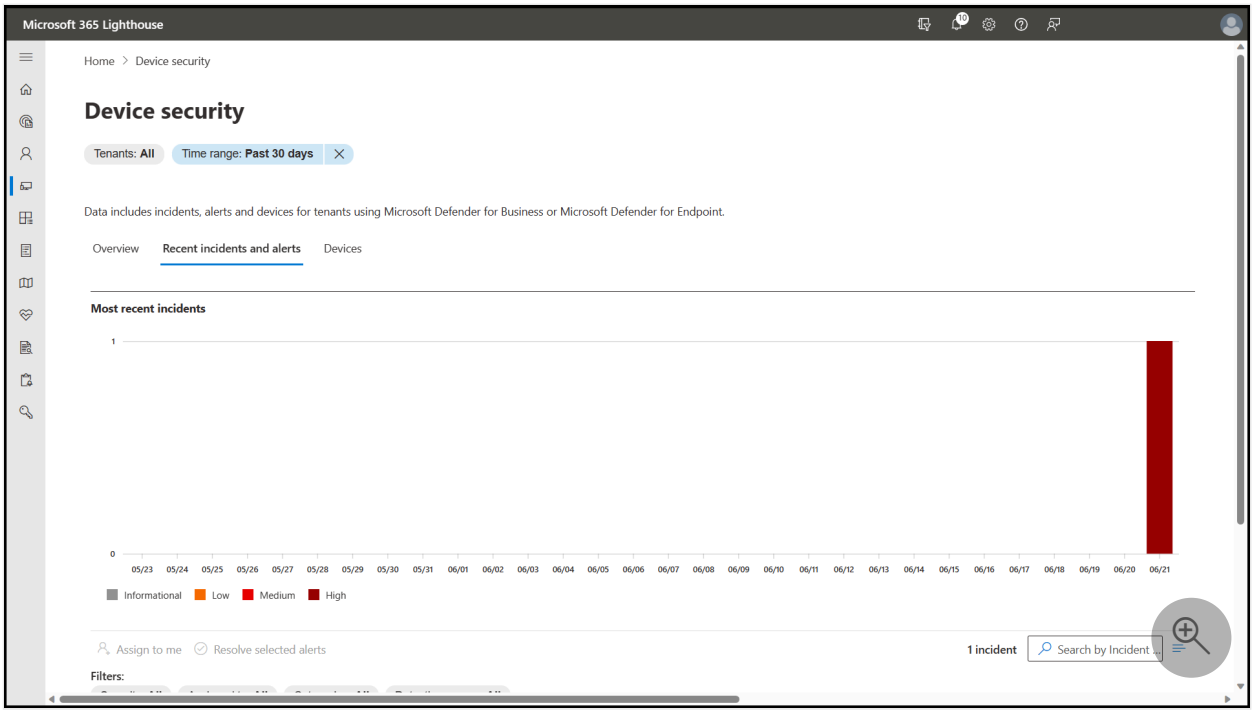
Microsoft Defender para punto de conexión proporciona seguridad de punto de conexión para proteger los dispositivos de los clientes frente a ransomware, malware, suplantación de identidad (phishing) y otras amenazas. Microsoft 365 Lighthouse le permite ver información e información de seguridad de los puntos de conexión para todos los inquilinos administrados.

Puede acceder a la página Seguridad del dispositivo en Microsoft 365 Lighthouse desde la tarjeta **Incidentes de seguridad** de la página Inicio o desde el panel de navegación izquierdo; para ello, seleccione **Dispositivos**>**Seguridad del dispositivo**. Verá los incidentes de seguridad y las alertas en los inquilinos que necesitan atención y los dispositivos que se han incorporado a Microsoft Defender para punto de conexión.

> ⓘ **Nota**
>
> En esta página se proporciona el número de inquilinos para los que los datos no están disponibles porque no tienen las licencias necesarias.

Pestaña Incidentes y alertas

La pestaña Incidentes y alertas proporciona una vista multiinquilino de incidentes y alertas que se marcaron desde dispositivos en la red de los clientes. De forma predeterminada, la pestaña muestra los incidentes activos detectados en los últimos 30 días. Puede seleccionar cualquier incidente o alerta para abrir el panel de detalles para ver más información. En el panel de detalles, también puede resolver el incidente o la alerta, o asignarlo usted mismo.

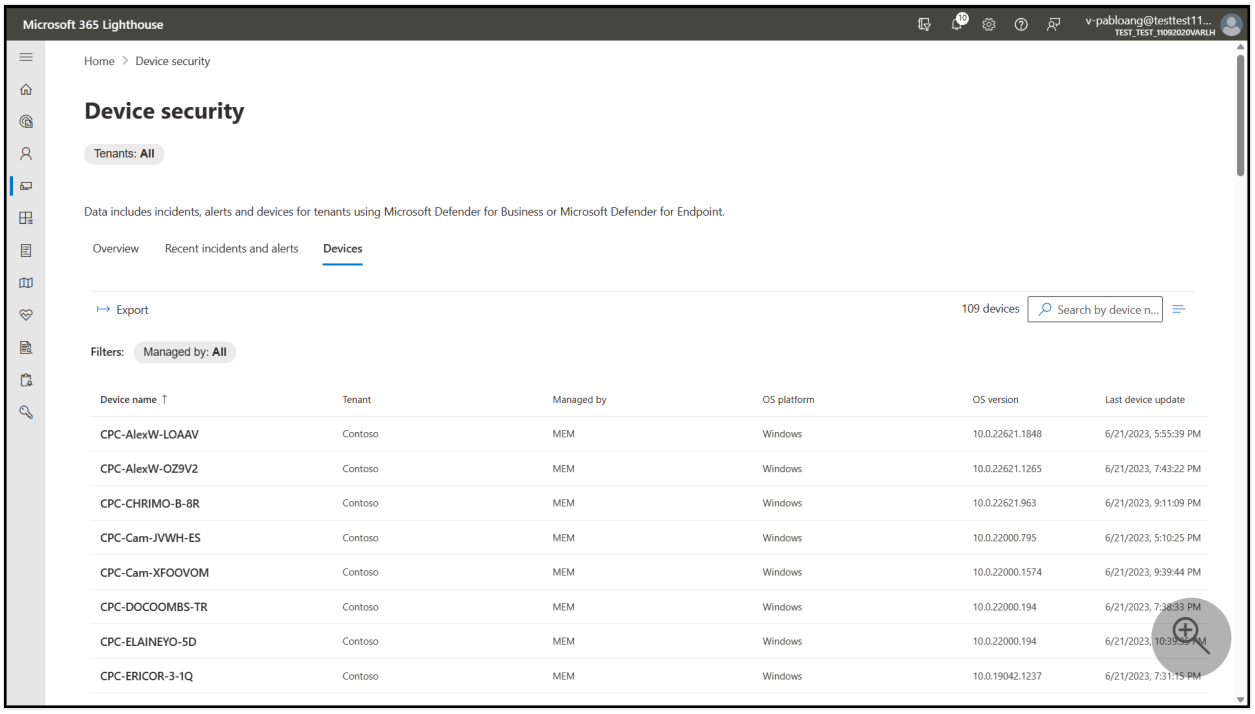


Pestaña Dispositivos

En la pestaña Dispositivos se enumeran todos los dispositivos de los inquilinos administrados que se han incorporado a Microsoft Defender para punto de conexión. Esta lista incluye dispositivos administrados por Microsoft Intune y Microsoft Defender para punto de conexión.

La pestaña Dispositivos también incluye las siguientes opciones:

- **Exportar**: seleccione esta opción para exportar los datos de cumplimiento de dispositivos a un archivo de valores separados por comas (.csv) de Excel.
- **Búsqueda**: escriba palabras clave para localizar rápidamente un dispositivo específico en la lista.



Contenido relacionado

Administración de incidentes de Microsoft Defender para punto de conexión (artículo)
Investigación de incidentes en Microsoft Defender para punto de conexión (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Introducción a la página de administración de vulnerabilidades en Microsoft 365 Lighthouse

Artículo • 04/06/2024

El faro de Microsoft 365 proporciona una vista multiinquilino de la puntuación de exposición y las recomendaciones de Administración de vulnerabilidades de Microsoft Defender en Microsoft Defender para empresas y Microsoft Defender para punto de conexión. La puntuación de exposición de Administración de vulnerabilidades de Microsoft Defender refleja lo vulnerables que son los inquilinos a las amenazas de ciberseguridad. La administración de vulnerabilidades de Microsoft Defender ayuda a identificar y crear de forma proactiva una base segura para los dispositivos a través de la corrección de vulnerabilidades de software y configuraciones incorrectas en entornos de cliente.

Para más información sobre la administración de vulnerabilidades, consulte ¿Qué es la administración de vulnerabilidades de Microsoft Defender?

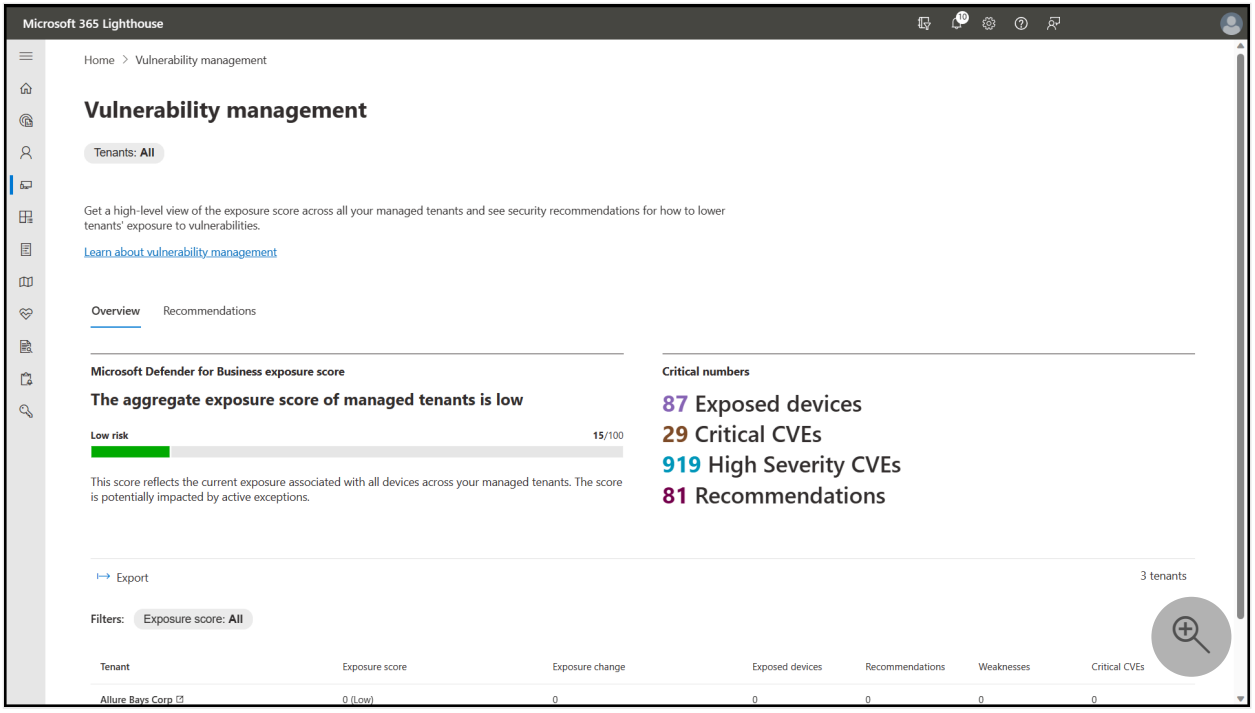
Puede acceder a la página Administración de vulnerabilidades de Lighthouse desde la tarjeta de **puntuación de exposición de Microsoft Defender para empresas** en la página **Inicio** o desde el panel de navegación izquierdo seleccionando **Administración de vulnerabilidades de dispositivos**>. Verá una vista multiinquilino de la exposición y las vulnerabilidades detectadas para todos los inquilinos que tienen dispositivos incorporados a Microsoft Defender para empresas o Microsoft Defender para punto de conexión.

> **Nota**
>
> En esta página se proporciona el número de inquilinos para los que los datos no están disponibles porque no tienen las licencias necesarias.

Pestaña da Información general

La pestaña información general proporciona información sobre varios inquilinos sobre la puntuación de exposición, el número de dispositivos expuestos, las vulnerabilidades y las recomendaciones para que los inquilinos reduzcan su exposición. Puede filtrar la lista por puntuación de exposición, nombre de inquilino o etiqueta de inquilino. Seleccione un inquilino de la lista que se va a llevar a la página del panel de administración de

vulnerabilidades de ese inquilino en el portal de Microsoft Defender. Para exportar datos de puntuación de exposición a un archivo de valores separados por comas (.csv) de Excel, seleccione **Exportar**.



Contenido relacionado

Qué es la administración de vulnerabilidades de Microsoft Defender (artículo)
Puntuación de exposición en Administración de vulnerabilidades de Defender (artículo)
Información general de la página Seguridad del dispositivo en Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Información general de la página Mensajes en cuarentena de Microsoft 365 Lighthouse

Artículo • 02/11/2024

Microsoft 365 Lighthouse permite ver información e información sobre los mensajes de correo electrónico en cuarentena en todos los inquilinos del cliente. Desde una sola vista, puede evaluar los mensajes de correo electrónico en cuarentena y realizar las acciones adecuadas. Los datos están disponibles si el inquilino ha implementado Exchange Online Protection (EOP) y Microsoft Defender para el plan 1 de Office365 (MDO).

Para acceder a la información de Lighthouse, seleccione **Inicio** en el panel de navegación izquierdo o seleccione **Mensajes en cuarentena** en el panel de navegación izquierdo para abrir la página **Mensajes en cuarentena** .

> ⓘ **Nota**
>
> En esta página se proporciona el número de inquilinos para los que los datos no están disponibles porque no tienen las licencias necesarias.

Página mensajes en cuarentena

En esta página, puede ver estadísticas consolidadas en los inquilinos de los clientes, datos de tendencia para el tipo y volumen de datos de cuarentena e información relacionada con las colas de cuarentena en inquilinos de clientes individuales.

La sección **Estado de los mensajes** proporciona una vista consolidada entre los inquilinos aptos incorporados actualmente a Lighthouse. La vista incluye

- Total de mensajes en cuarentena
- Total de mensajes en espera de revisión
- Mensajes que se aproximan actualmente al límite de cuarentena predeterminado de 30 días y que están a punto de quitarse automáticamente (expiran)
- Mensajes que se han liberado de la cuarentena
- Número total de buzones afectados en todos los inquilinos

Los datos reflejan los últimos 30 días; sin embargo, puede usar el filtro **Intervalo de tiempo** para modificar la vista.

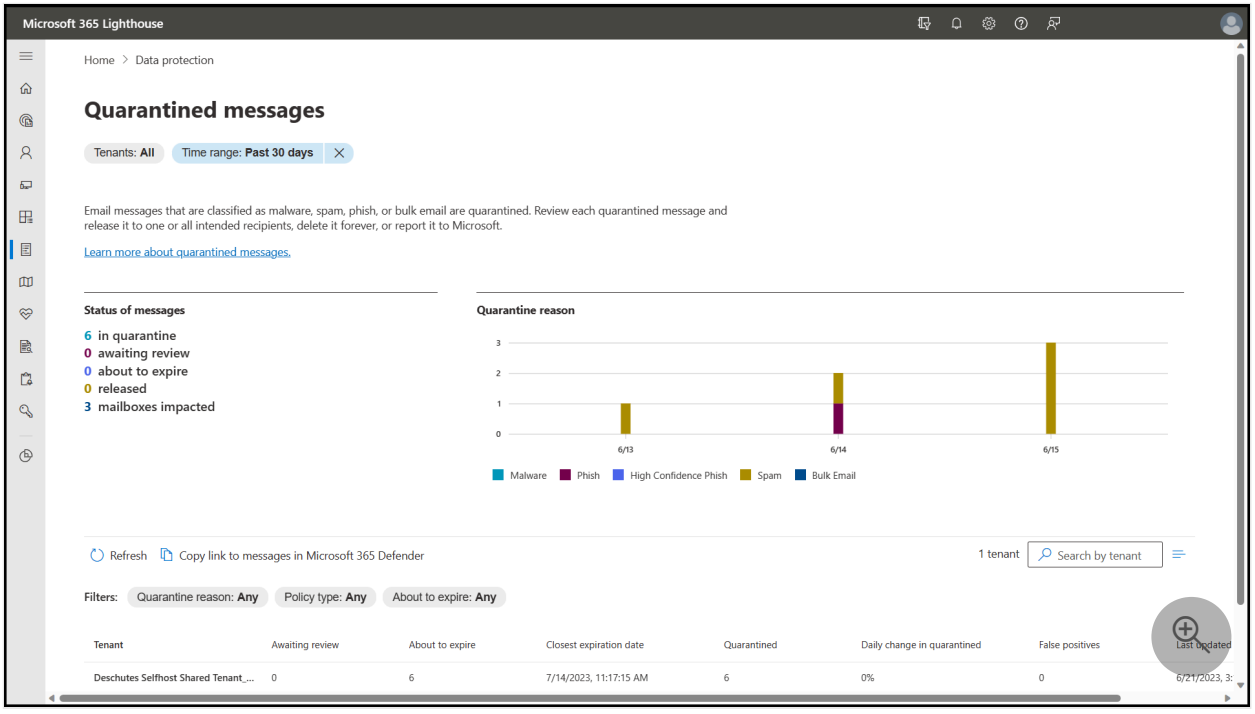
La sección **Motivo de cuarentena** contiene un desglose de los recuentos de cuarentena por Exchange Online Protection (EOP) y Microsoft Defender para el tipo de directiva plan 1 (MDO) de Office365. Estos tipos incluyen

- Malware
- Suplantación de identidad (phishing)
- Suplantación de identidad de alta confianza
- Correo no deseado
- Email masivas

La lista de cuarentena es una vista ordenable de la información de cuarentena por inquilino. En esta vista, puede filtrar por la siguiente información:

- **Motivo de cuarentena:** Cualquiera, Malware, Phish, Phish de alta confianza, Spam, Bulk Email
- **Tipo de directiva:** Cualquiera, Antimalware, Anti-phishing, Anti-spam, Datos adjuntos seguros, Regla de transporte, Desconocido
- **A punto de expirar:** Cualquiera, Hoy, dentro de dos días, dentro de siete días

También puede ajustar las columnas y ordenar los datos en función del inquilino, el estado del mensaje y las fechas de expiración.



La opción **Copiar vínculo a mensajes en Microsoft365 Defender** proporciona un vínculo a Microsoft Defender portal donde puede acceder a la cola de cuarentena de correo electrónico de su inquilino y administrarla. Debe autenticarse para poder realizar cualquier acción.

Contenido relacionado

Mensajes de correo electrónico en cuarentena (artículo)
Recomendaciones de Microsoft para la configuración de seguridad de EOP y Defender para Office 365 (artículo)
Introducción a Exchange Online Protection (EOP) (artículo)
Información general de la página Administración de amenazas (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Información general de la página Aplicaciones de Microsoft 365 Lighthouse

Artículo • 21/06/2023

Microsoft 365 Lighthouse incluye las características de Microsoft Endpoint Analytics para aplicaciones en una vista de administración simplificada. La página Aplicaciones proporciona información sobre los posibles problemas de las aplicaciones de escritorio en dispositivos administrados. Puede identificar rápidamente las principales aplicaciones que afectan a la productividad del usuario final junto con las métricas de error de aplicaciones para estas aplicaciones.

Los datos solo reflejan dispositivos Windows totalmente administrados. No se admiten los datos de Bring Your Own Devices.

Requisitos

Los dispositivos deben inscribirse en Microsoft Intune. Para obtener más información sobre la inscripción, consulte ¿Qué es Análisis de puntos de conexión? Una vez inscrito un dispositivo, la página Aplicaciones se rellena automáticamente con datos. Las actualizaciones pueden tardar hasta 48 horas.

> ⓘ **Nota**
>
> Si los datos no se muestran para una aplicación específica, compruebe que la directiva está habilitada. En el plan de implementación del inquilino, en **Configurar la inscripción de dispositivos**, compruebe que la **directiva de supervisión del estado** del dispositivo es compatible. Si no es compatible, implemente la directiva.

Pestaña de rendimiento de la aplicación

La pestaña Rendimiento de las aplicaciones proporciona información de la aplicación de los últimos 14 días. Para cada aplicación, Lighthouse proporciona la siguiente información,

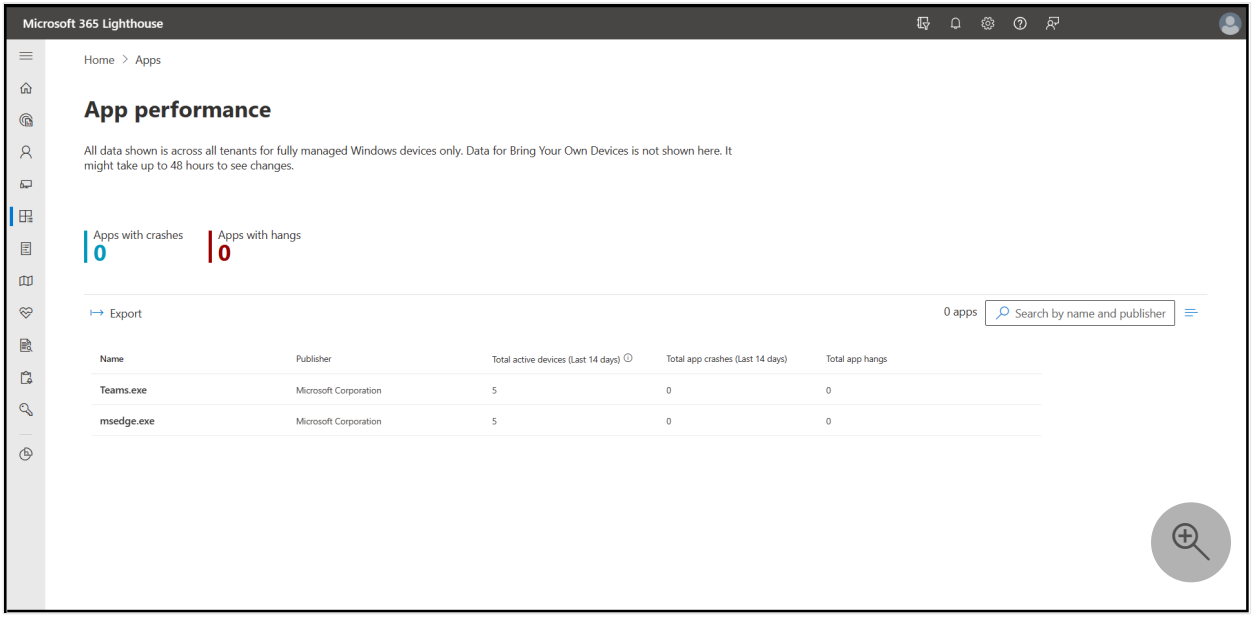
- **Nombre**: identificador de la aplicación en el manifiesto de archivo proporcionado por los dispositivos cliente. El nombre de la aplicación suele estar en formato ejecutable (o .exe).

- **Publicador**: publicador del ejecutable notificado en el manifiesto de archivo.
- **Totalde dispositivos activos (14 días):** el número total de dispositivos inscritos que han iniciado esta aplicación al menos una vez en los últimos 14 días.
- **Total de bloqueos (14 días):** Número total de eventos de bloqueo de aplicaciones notificados en todos los dispositivos inscritos en los últimos 14 días.
- **Total de bloqueos de aplicaciones:** El número total de bloqueos de aplicación notificados en todos los dispositivos inscritos en los últimos 14 días.

Seleccione una aplicación de la lista para obtener información más detallada sobre la aplicación, incluidos los dispositivos que tienen problemas. Se proporciona un acceso directo para ver el dispositivo en Microsoft Endpoint Manager, donde puede ver más información y recomendaciones.

La pestaña Rendimiento de la aplicación también incluye las siguientes opciones:

- **Exportar**: seleccione esta opción para exportar los datos de rendimiento de la aplicación a un archivo de valores separados por comas (.csv) de Excel.
- **Buscar**: escriba palabras clave para localizar rápidamente un nombre o publicador específico en la lista.



Contenido relacionado

¿Qué es el análisis de punto de conexión? (artículo)
Confiabilidad de aplicaciones en análisis de puntos de conexión (artículo)
Información general de la página Estado del dispositivo en Microsoft 365 Lighthouse (artículo)

Introducción al Asesor de ventas en Microsoft 365 Lighthouse

Artículo • 22/07/2023

Sales Advisor es una experiencia de administración del ciclo de vida del cliente (CLM) que proporciona información sobre los clientes controlada por IA, recomendaciones útiles y orientación prescriptiva a lo largo del ciclo de vida del cliente. Sales Advisor se basa en un conjunto de reglas de negocio, uso del cliente y posiciones de licencia. Permite una técnica denominada "modelado de propensión" para presentar oportunidades dinámicas para que los asociados adquieran, conserven y aumenten mejor sus clientes.

Para ver Sales Advisor, seleccione **Oportunidades de Sales Advisor** > en el panel de navegación izquierdo de Lighthouse.

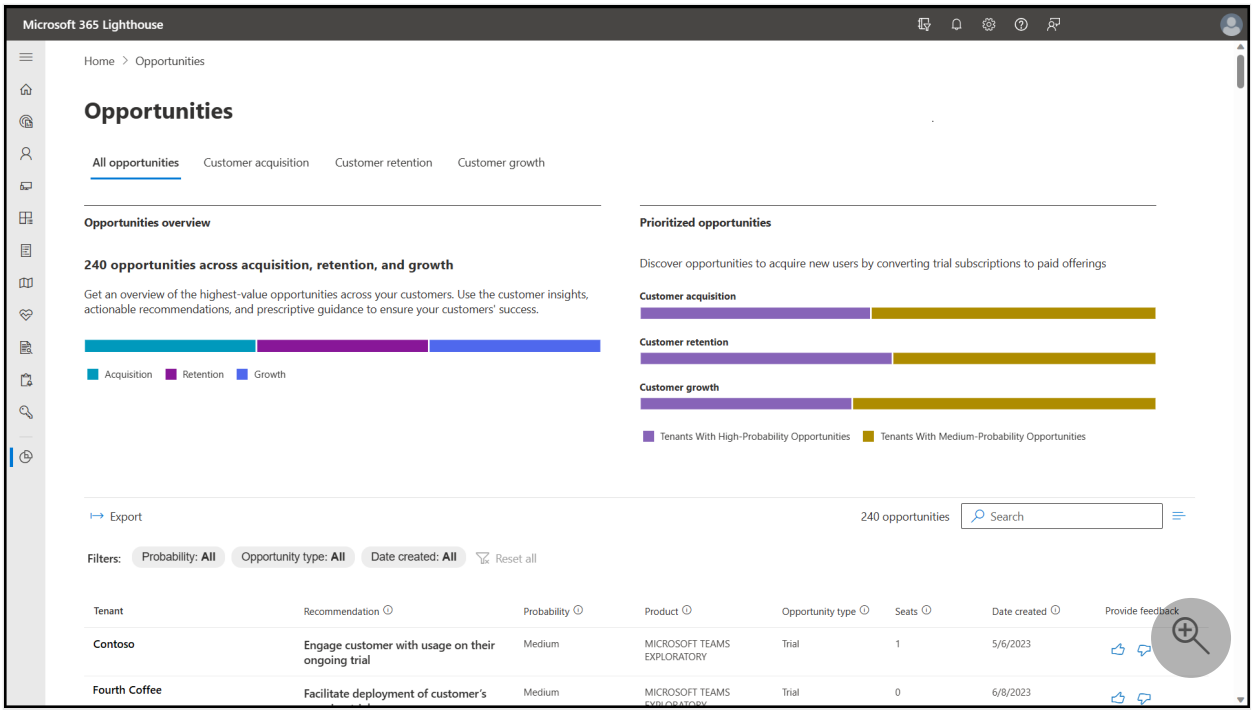
IMPORTANTE: Para usar Sales Advisor, los usuarios deben tener los roles adecuados enumerados en Obtener acceso a Sales Advisor.

Vea: ¿Qué es Sales Advisor?

Vídeo: Versión preliminar: Microsoft 365 Lighthouse Aviso de ventas

Ventajas de Sales Advisor

Garantice el éxito de los clientes mediante la información de los clientes basada en la inteligencia artificial, recomendaciones accionables e instrucciones prescriptivas. Maximice la inversión de sus clientes en Microsoft 365 y ofrezca valor en cada fase de su recorrido.



- **Comprenda mejor a los clientes**: Sales Advisor analiza el comportamiento, las preferencias, las necesidades y los comentarios de los clientes en varios canales y orígenes. Le ofrece una visión holística de la salud y los intereses de sus clientes, para que pueda adaptar su comunicación y ofertas en consecuencia.
- **Nutrir a los clientes de forma proactiva:** Sales Advisor identifica las mejores oportunidades para interactuar con sus clientes en función de su valor, riesgo y preparación potenciales. Le ayuda a priorizar sus acciones y alcance, para que pueda centrarse en las actividades más impactantes que pueden impulsar la retención, el crecimiento y la promoción.
- **Ofrecer valor de forma coherente**: Sales Advisor le guía por los procedimientos recomendados y los pasos necesarios para ofrecer valor a los clientes a lo largo de su ciclo de vida. Le ayuda a alinear sus ofertas con sus objetivos y desafíos, a demostrar las ventajas de sus soluciones y a abordar cualquier problema o problema de forma eficaz.
- Identifique al cliente adecuado con el que interactuar en el momento adecuado.
- Reciba una advertencia temprana de los clientes que están en riesgo de abandono.
- Aproveche la información contextual para comprender mejor la oportunidad.
- Conozca a sus clientes y dónde se encuentran en su recorrido por la nube.
- Aproveche las recomendaciones de procedimientos recomendados de Microsoft.
- Acceda a recursos específicos de oportunidades para impulsar la acción.

Idiomas disponibles

Sales Advisor se ofrece en varios idiomas. En aquellos países en los que no aparece el idioma local, la reserva es inglés, pero el Centro de partners permite al usuario establecer su idioma preferido. Es posible que haya más idiomas disponibles en el futuro.

Sales Advisor admite actualmente los siguientes idiomas:

- Inglés (Estados Unidos)
- Francés (Francia)
- Español (España)
- Alemán
- Italiano
- Coreano
- Neerlandés
- Portugués (Brasil)
- Turco

Privacidad

Sales Advisor se ofrece en varios idiomas. En aquellos países en los que no aparece el idioma local, la reserva es inglés, pero el Centro de partners permite al usuario establecer su idioma preferido. Es posible que haya más idiomas disponibles en el futuro.

Sales Advisor admite actualmente los siguientes idiomas:

- Inglés (Estados Unidos)
- Francés (Francia)
- Español (España)
- Alemán
- Italiano
- Coreano
- Neerlandés
- Portugués (Brasil)
- Turco

Obtención de acceso a Sales Advisor

Para usar Sales Advisor, debe tener el rol Visor de informes ejecutivos o Visor de informes en el Centro de partners. Para obtener más información, consulte Obtención de acceso a Sales Advisor.

Contenido relacionado

Obtener acceso a Sales Advisor (artículo)
Descripción de oportunidades y datos en Sales Advisor (artículo)
Microsoft 365 Lighthouse – Transformación (Blog)

Obtener acceso a Sales Advisor en Microsoft 365 Lighthouse

Artículo • 20/01/2025

En este artículo se proporcionan instrucciones sobre cómo registrarse para Microsoft 365 Lighthouse Sales Advisor. Incluso si tiene acceso a Lighthouse, se requiere un rol adicional en el Centro de partners para obtener acceso a Sales Advisor.

Sales Advisor está diseñado para vendedores. Los roles orientados al cliente en la organización del asociado que se centran en el desarrollo empresarial, el éxito del cliente y las ventas pueden beneficiarse del acceso directo a la experiencia del asesor de ventas.

Antes de empezar

- El inquilino del asociado debe incorporarse a Microsoft 365 Lighthouse.
- Debe tener el rol Administrador de cuentas en Lighthouse. Si no tiene el rol Administrador de cuentas, póngase en contacto con alguien que tenga el rol Administrador en Lighthouse y pídale que le asigne el rol.

Roles adecuados en el Centro de partners

- El rol visor de informes ejecutivo proporciona acceso a todos los conjuntos de datos de informes.
- El rol Visor de informes proporciona acceso a la mayoría de los conjuntos de datos de informes, pero no a datos confidenciales, como los ingresos y la información personal del cliente o empleado.
- Debe tener al menos el rol De administrador de cuenta para asignar a los usuarios los roles mencionados anteriormente, que se asignan para toda una empresa o para una ubicación específica del Programa de partners en la nube de Microsoft.

Para obtener más información, vea Acceso basado en rol de CPP: Centro de partners.

Obtener acceso a Sales Advisor

1. Vaya al Centro de partners de Microsoft 365 en https://partner.microsoft.com/dashboard/home.

2. Vaya a **Configuración de la cuenta Administración**>**de usuarios**.

3. En **Usuarios**, seleccione la cuenta de usuario para editar los permisos.
4. En **Detalles del usuario**, vaya a **Roles aplicables a los programas asociados** y seleccione **Ver datos e informes para una o varias ubicaciones (seleccione las ubicaciones donde el usuario necesita poder ver los datos y los informes).**
5. Asigne **el rol Visor de informes** o **Visor de informes ejecutivos** mediante uno de los dos métodos.

- Seleccione **Toda la organización** si desea que el usuario tenga acceso a todas las ubicaciones enumeradas más otras ubicaciones nuevas que se agregarán en el futuro.
- Seleccione **una o varias ubicaciones enumeradas a continuación** y asigne **visor de** informes o **visor de informes ejecutivos** en la lista desplegable de la columna Roles del visor de informes para conceder acceso por ubicación.

Pasos siguientes

Una vez que tenga acceso a Sales Advisor, puede empezar a revisar información en la página Oportunidades. En el panel de navegación izquierdo de Lighthouse, seleccione **Oportunidades de Sales Advisor**>. Para obtener más información sobre las oportunidades, consulte Descripción de oportunidades y datos en Sales Advisor.

Contenido relacionado

Información general de Sales Advisor (artículo)
Descripción de oportunidades y datos en Sales Advisor (artículo)
Acceso basado en rol de CPP: Centro de partners (artículo)
Roles con acceso al panel de Insights: Centro de partners (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Descripción de oportunidades y datos en Sales Advisor en Microsoft 365 Lighthouse

Artículo • 22/07/2023

Sales Advisor se centra en generar recomendaciones que ayuden a impulsar las conversaciones que los asociados tienen con los clientes a lo largo del ciclo de vida del cliente. Usa modelos de aprendizaje automático (ML) para proporcionar acciones recomendadas y el razonamiento detrás de cada recomendación. Los datos usados en los modelos combinan información sobre el cliente, las suscripciones actuales y el uso y la interacción de cada producto.

Los modelos de aprendizaje automático actuales recomiendan oportunidades de crecimiento, retención y adquisición.

Oportunidades

Las oportunidades son recomendaciones específicas y procesables generadas por Sales Advisor. Cada oportunidad contiene una recomendación para un cliente determinado, conclusiones, acciones sugeridas, recursos, suscripciones y datos de uso que le guiarán. Cada oportunidad contiene los siguientes datos:

- Cliente: nombre del cliente
- Recomendación: Acción recomendada para esta oportunidad
- Estado de probabilidad: probabilidad de que una predicción sea correcta. Los valores posibles son Alto, Medio o Bajo.
- Tipo de oportunidad: indica la categoría general de oportunidades que se presentan.
    - Adquisición de clientes
    - Retención de clientes
    - Crecimiento del cliente
- Producto: producto asociado a la oportunidad (no visible para las oportunidades de retención del cliente)

- Puestos: número de licencias de pago en el inquilino del cliente
- Fecha agregada o creada: fecha en que se creó la oportunidad por primera vez para el cliente. Las recomendaciones se actualizan periódicamente para capturar las señales de cliente más recientes, por lo que seguirá apareciendo una oportunidad si las señales del cliente siguen siendo las mismas, independientemente de cuándo se creó por primera vez.

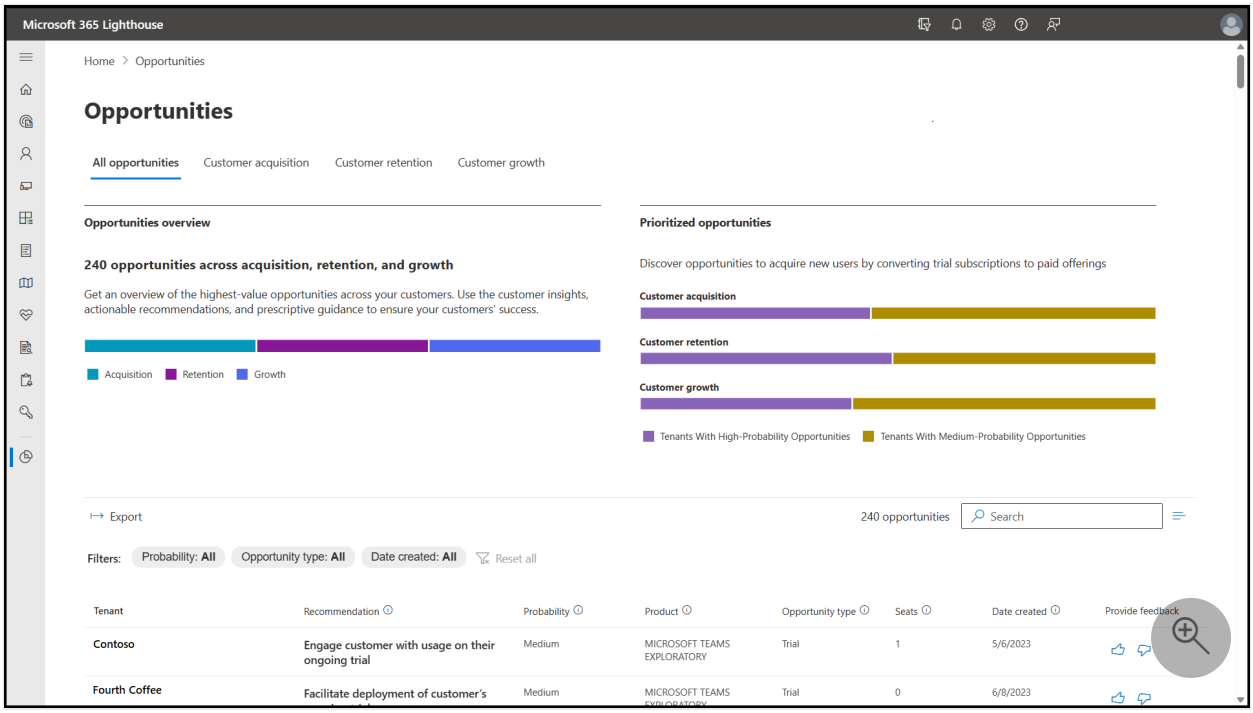
NOTA: Cada cliente puede tener cero, una o más oportunidades. Solo los clientes con una o más oportunidades se rellenarán en la tabla de oportunidades. Dentro de cada tipo de oportunidad, solo habrá una oportunidad por cliente.

Página Oportunidades

La página Oportunidades muestra oportunidades en todos los tipos de oportunidades, adquisición de clientes, retención de clientes y crecimiento del cliente. En la página Oportunidades se resumen las oportunidades de mayor valor dentro de la base de instalación de Microsoft 365 de un asociado. La pestaña **Todas las oportunidades** se divide en tres áreas:

- **Introducción a las oportunidades** : una vista de resumen que contiene el número total de inquilinos de clientes y el número de oportunidades por tipo de oportunidad.
- **Oportunidades prioritarias** : una vista resumida que desglosa el número de oportunidades de alta propensión y las oportunidades de propensión media por tipo de oportunidad.
- **Tabla de recomendaciones** : contiene Inquilino del cliente, Recomendación, Estado de probabilidad, Tipo de oportunidad, Asientos, Fecha agregada y Proporcionar comentarios. De forma predeterminada, la tabla se ordena para mostrar primero la recomendación más reciente. La vista de tabla de recomendaciones muestra cada oportunidad como una fila independiente.

Las pestañas **Adquisición de clientes**, **Retención de clientes** y **Crecimiento del cliente** son una vista de los mismos datos de oportunidad filtrados por categoría de oportunidad.



La página Oportunidades también incluye las siguientes opciones:

- **Exportar:** Seleccione esta opción para exportar datos de oportunidades a un archivo de valores separados por comas (.csv) de Excel.
- **Búsqueda:** Escriba palabras clave para localizar rápidamente un inquilino específico en la lista.

Categoría de oportunidad

Hay tres categorías de oportunidades para cubrir las fases del ciclo de vida de un cliente: adquisición de clientes, retención de clientes y crecimiento del cliente. Estos tipos se alinean con las tres pestañas de la página Oportunidades.

Adquisición de clientes

Tipo de oportunidad diseñado para acelerar la adquisición de clientes mediante pruebas y conversaciones de conversión de prueba para vender Microsoft 365 de forma más eficaz. Los partners pueden detectar oportunidades para adquirir nuevos usuarios mediante la conversión de suscripciones de prueba a ofertas de pago.

Retención de clientes

Tipo de oportunidad que está diseñado para obtener advertencias tempranas en las que la interacción directa puede evitar la renovación futura de Microsoft 365 para servir

mejor y retener a los clientes. Los asociados pueden detectar oportunidades para aumentar la adopción y mitigar el riesgo de abandono de los clientes.

Crecimiento del cliente

Tipo de oportunidad diseñado para saber qué clientes están listos para el siguiente paso de su transformación digital en función de los patrones de uso y comportamientos de clientes similares. Los partners pueden detectar oportunidades para hacer crecer su negocio mediante la actualización de los clientes a suscripciones de mayor valor.

Modelos disponibles por tipo de oportunidad

A continuación se muestran los modelos de datos disponibles actualmente en Sales Advisor como recomendaciones por categoría de oportunidad.

Modelo de oportunidad	**Categoría de oportunidad**	**Basado en**	**SKU o productos cubiertos**
B-SKU: SKU empresariales de Microsoft 365	Crecimiento del cliente	Aprendizaje automático	Independiente, Business Basic, Business Standard, Business Premium
E-SKU: SKU de Microsoft 365 Enterprise	Crecimiento del cliente	Aprendizaje automático	Office 365 E3, Microsoft 365 E3, Microsoft 365 E5, EMS E5
Riesgo de abandono	Retención de clientes	Aprendizaje automático	Core Apps, Teams, SMB Tenants
Interacción de inquilinos SMB	Retención de clientes	Regla de negocio	Email, Core Apps, Teams, SharePoint, OneDrive para la Empresa
Recomendación de crecimiento de MDO	Crecimiento del cliente	Árbol de decisión	Microsoft 365 Empresa Premium o Microsoft Defender para Office 365 P2
Recomendación de interacción de MFA	Interacción con el cliente	Árbol de decisión	Multi-Factor Authentication en Azure AD
Recomendación de crecimiento de MDB	Crecimiento del cliente	Árbol de decisión	Microsoft Defender para Empresas (MDB)
Ensayos	Adquisición de clientes	Regla de negocio	Teams Exploratory

Terminología del Asesor de ventas

En la lista siguiente se proporcionan términos y definiciones importantes que se usan en Sales Advisor.

Término	Definición
Uso activo	Uso activo agrega el número de usuarios o dispositivos activos en función de acciones intencionadas, que varía en cada aplicación. Los datos de uso activos pueden ayudar a calcular métricas de uso, como usuarios activos diarios (DAU) y usuarios activos mensuales (MAU).
Usuarios activos	Número de usuarios que usan activamente la carga de trabajo.
Usuarios asignados	Número de puestos que contienen la carga de trabajo asignada a un usuario.
Adquisición de clientes	Categoría de oportunidad diseñada para acelerar la adquisición de clientes mediante pruebas y conversaciones de conversión de prueba para vender Microsoft 365 de forma más eficaz.
Crecimiento del cliente	Categoría de oportunidad diseñada para saber qué clientes están listos para el siguiente paso de su transformación digital en función de los patrones de uso y comportamientos de clientes similares.
Información del cliente	Las características del cliente seleccionado en función de los datos históricos y la correlación explican por qué se sugiere la recomendación específica.
Retención de clientes	Categoría de oportunidad diseñada para obtener advertencias tempranas en las que la interacción directa puede evitar la renovación futura de Microsoft 365 para servir mejor y retener a los clientes.
Información de uso del cliente	Pestaña del control flotante Recomendación del cliente que muestra cómo los usuarios usan los servicios de Microsoft 365 para todos los productos que pertenecen. El gráfico muestra el uso por usuario y la tabla muestra el número de usuarios asignados, los usuarios activos y las tendencias.
Clientes con oportunidades	Resumen de los clientes que tienen una o varias oportunidades.
Oportunidad	Las oportunidades son acciones específicas y accionables generadas a partir del modelado de propensión del Asesor de ventas. Cada oportunidad contiene una recomendación para un cliente determinado, información, acciones sugeridas, recursos, suscripciones y datos de uso para guiar al asociado.
Categoría de oportunidad	Tipo de oportunidad. Hay tres categorías de oportunidades: Adquisición de clientes, Retención de clientes y Crecimiento del cliente. Indica la categoría general de oportunidades presentadas.

Término	Definición
Oportunidades por categoría	Resumen de oportunidades en la fase del ciclo de vida del cliente (adquisición del cliente, retención de clientes, crecimiento del cliente).
Estado de probabilidad	Probabilidad de que la predicción sea correcta, con valores posibles de Alto o Bajo.
Producto	Producto de Microsoft asociado a la oportunidad.
Recomendación	Acción recomendada para esta oportunidad.
Recursos	Dentro de una recomendación del cliente, los recursos son documentos como un cuaderno de estrategias, una demostración, hojas de referencia rápida y plantillas de correo electrónico para ayudar a preparar a los asociados para la conversación con el cliente con respecto a la oportunidad.
Asientos	Número de licencias de pago en el inquilino del cliente.
Suscripciones	Pestaña del control flotante Recomendación del cliente que muestra el nombre del producto, la cantidad adquirida y el estado de suscripción de los productos comprados por el cliente de la organización del asociado o de Microsoft directamente.
Acciones recomendadas	Se recomiendan acciones específicas, como la ejecución de un taller, para aplicar la recomendación.
Tendencia	Tendencia en el uso activo mensual de los tres meses anteriores. Sin cambios, positivos o negativos.
Uso por usuario	Historial del uso mensual activo por carga de trabajo
Carga de trabajo	Exchange Online, OneDrive para la Empresa, SharePoint Online, Microsoft Teams, etc.

Preguntas más frecuentes para Sales Advisor

Consulte la sección Administración de oportunidades con Sales Advisor de preguntas más frecuentes (P+F) para obtener más información sobre Sales Advisor.

Contenido relacionado

Visualización de oportunidades en Sales Advisor (artículo)
Información general de Sales Advisor (artículo)

Visualización de oportunidades en Sales Advisor en Microsoft 365 Lighthouse

Artículo • 28/09/2024

Sales Advisor proporciona recomendaciones accionables para administrar el cliente y hacer crecer su negocio. Para comprender cuál es una oportunidad, consulte Descripción de las oportunidades y los datos en Sales Advisor.

Cada cliente puede tener cero, una o más oportunidades. Solo los clientes con una o más oportunidades se rellenan en la tabla de oportunidades. Dentro de cada tipo de oportunidad, solo habrá una oportunidad por cliente.

Antes de empezar

Debe tener el rol Visor de informes ejecutivos o Visor de informes en el Centro de partners para acceder a Sales Advisor. Para obtener más información, consulte Obtención de acceso a Sales Advisor.

Visualización de oportunidades

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Oportunidades de Sales Advisor**>.
2. En la pestaña **Todas las oportunidades** , seleccione el inquilino que desea investigar.
3. En el panel de detalles del inquilino, revise cada una de las pestañas para obtener detalles específicos del inquilino y la posible acción.

Expandir tabla

Pestaña	Descripción
Recomendación	Contiene lo siguiente: **Información del cliente** : características del cliente seleccionado en función de los datos históricos y la correlación, explica por qué se sugiere la recomendación específica. **Acciones sugeridas** : sugerencias específicas para aplicar la recomendación (por ejemplo, ejecutar un taller). **Recursos relacionados:** materiales de marketing como cuadernos de estrategias, demostraciones, hojas de referencia rápida y plantillas de correo

Pestaña	Descripción
	electrónico para ayudar a preparar a los asociados para la conversación con el cliente con respecto a la oportunidad.
Suscripción	Contiene información de suscripción sobre los productos comprados por el cliente de la organización del asociado o de Microsoft directamente, incluidos el nombre del producto, la cantidad de compra y el estado de la suscripción (activo/inactivo).
Uso	Muestra cómo los usuarios usan los servicios de Microsoft 365 para todos los productos que posee el cliente. Incluye un gráfico de uso por usuario que se puede filtrar por carga de trabajo. Además, una vista de tabla con la siguiente información: **Carga de trabajo**: Exchange Online, OneDrive para la Empresa, Microsoft Entra ID, etc. **Usuarios asignados** : número de puestos que contienen la carga de trabajo asignada a un usuario. **Usuarios activos** : número de usuarios que usan activamente la carga de trabajo. **Tendencia** : la tendencia en el uso activo mensual de los tres meses anteriores se define como Sin cambio, Positivo o Negativo.

Visualización de oportunidades por tipo de oportunidad

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Oportunidades de Sales Advisor**>.
2. Seleccione el tipo de oportunidad deseado que desea revisar.

Para obtener una definición de cada tipo de oportunidad, consulte la sección Tipo de oportunidad en Descripción de oportunidades y datos en Sales Advisor.

Exportación de oportunidades de Sales Advisor

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Oportunidades de Sales Advisor**>.
2. Seleccione la vista que desea exportar (Todas las oportunidades, Adquisición de clientes, Retención de clientes o Crecimiento del cliente).
3. Filtre la lista según sea necesario mediante los filtros (Probabilidad, Tipo de oportunidad y Fecha de creación).
4. Seleccione **Exportar**.

Lighthouse exporta los datos mostrados en un archivo CSV que puede integrar en herramientas internas y crear informes personalizados. Si ha aplicado filtros a la tabla, los datos exportados reflejan los filtros seleccionados. El archivo CSV descargado contiene los datos siguientes:

- Id. de cliente
- TPID
- Nombre del cliente
- Tipo de oportunidad
- Información del cliente
- Acciones recomendadas
- Recursos relacionados
- Propensión al crecimiento
- Producto recomendado
- Asientos
- Fecha agregada
- Vínculo (una dirección URL única para cada oportunidad)

Contenido relacionado

Información general de Sales Advisor (artículo)
Obtener acceso a Sales Advisor (artículo)
Descripción de oportunidades y datos en Sales Advisor (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Obtenga ayuda y soporte técnico para Microsoft 365 Lighthouse

Artículo • 31/08/2024

Hay varias opciones disponibles si necesita ayuda. En primer lugar, compruebe si hay problemas conocidos:

- Revise el estado actual de los servicios de inquilino del cliente:

    1. En el panel de navegación izquierdo de Lighthouse, seleccione **Estado del servicio**.
    2. Vea información detallada sobre los problemas actuales y pasados.

- Revise el estado actual de los servicios de inquilino de Lighthouse:

    1. Vaya a la Centro de administración de Microsoft 365 en https://admin.microsoft.com.
    2. En el panel de navegación izquierdo, seleccione **Estado** > **Estado del servicio**.
    3. En la lista de servicios, busque **El conjunto de aplicaciones de Microsoft 365** y expándalo para mostrar todos los servicios del conjunto.
    4. Busque **Microsoft 365 Lighthouse** y compruebe el estado.

- Vea si el problema aparece en Problemas conocidos con Microsoft 365 Lighthouse.

Si experimenta un problema que no aparece en ninguno de estos recursos, siga las instrucciones de este artículo para ver las opciones de autoayuda o para crear una solicitud de servicio.

Antes de empezar

- Para crear y administrar solicitudes de servicio, debe tener al menos un rol de Microsoft Entra asignado con la siguiente propiedad establecida: **microsoft.office365.supportTickets/allEntities/allTasks**. Para obtener una lista de Microsoft Entra roles, consulte Microsoft Entra roles integrados. Para obtener información sobre cómo asignar roles, consulte Asignación de roles Microsoft Entra a los usuarios.

- Si necesita crear una solicitud de servicio, recopile tantos detalles como sea posible sobre el problema, como registros de diagnóstico, identificador de inquilino e identificadores de usuario (si se ven afectados usuarios específicos).

Acceso a ayuda y soporte técnico

1. En Lighthouse, seleccione el icono **?** en la parte superior del portal o el widget **de soporte técnico & ayuda** en la esquina inferior derecha del portal para abrir el panel **Ayuda** y, a continuación, realice una de las siguientes acciones:

    - Si está en la página del portal donde se produjo el problema, seleccione **Mostrar diagnóstico**.

      Esto creará un archivo JSON con información para ayudar a los agentes de soporte técnico a solucionar el problema. Guarde el archivo para que pueda adjuntarlo a la solicitud de servicio.

      > ⓘ **Nota**
      >
      > El archivo JSON contendrá información de identificación personal.

    - Si el problema no está aislado en la página actual del portal, vaya al paso siguiente.

2. En el panel **Ayuda** , seleccione el botón **Ayuda y soporte técnico** . Se abrirá el panel **¿Cómo podemos ayudar?**

    > ⓘ **Nota**
    >
    > Si el panel **¿Cómo podemos ayudar?** no se abre, deberá ponerse en contacto con un administrador del inquilino del asociado y pedirle ayuda.

3. En el panel **¿Cómo podemos ayudar?** , escriba una descripción del problema y, a continuación, presione **Entrar**. Se recomienda incluir el nombre completo *del producto Microsoft 365 Lighthouse* en la descripción para asegurarse de que los resultados de la búsqueda incluyan artículos de ayuda pertinentes.

4. Consulte la lista de artículos recomendados para ver si alguno de ellos ayuda a resolver el problema.

    Si escribe una descripción del problema y no devuelve una lista de artículos de ayuda, vuelva a escribir la descripción y pruebe otra búsqueda.

5. Si los artículos recomendados no ayudan, seleccione **Ponerse en contacto con soporte técnico**.

6. Rellene la información del formulario, adjunte las capturas de pantalla y el archivo JSON que guardó en el paso 1, si procede, y, a continuación, seleccione **Ponerse en contacto conmigo**. El tiempo de espera esperado se indica en el panel.

Contenido relacionado

Visualización del estado del servicio de inquilinoProblemas conocidos con Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)
Solución de problemas y resolución de problemas y mensajes de error en Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Problemas conocidos con Microsoft 365 Lighthouse

Artículo • 31/10/2024

En este artículo se enumeran los problemas conocidos de Microsoft 365 Lighthouse por área de características. Para obtener más información sobre Lighthouse, consulte Información general de Microsoft 365 Lighthouse.

Usuarios

Expandir tabla

Problema	Descripción	Solución
No se muestra ningún dato en la pestaña OneDrive del panel de detalles del usuario	Cuando un técnico de MSP intenta ver los datos de OneDrive en la pestaña OneDrive en el panel de detalles del usuario, ve el mensaje: "OneDrive no está configurado para este usuario. Pida a la persona que vaya a portal.office.com/onedrive para configurarlo. Puede tardar un tiempo. Si sigue viendo este mensaje 24 horas más tarde, póngase en contacto con el soporte técnico."	La pestaña OneDrive no admite la autenticación delegada en este momento. Para solucionar el problema, los técnicos de MSP deben ver los datos de OneDrive en el Centro de administración de Microsoft 365 iniciando sesión con las credenciales del cliente.

Administración de amenazas

Expandir tabla

Problema	Descripción	Solución
Falta el nombre de la amenaza	Cuando los técnicos de MSP ven la lista de amenazas desde la página Administración de amenazas, es posible que falte el nombre de la amenaza en algunas amenazas. Esto ocurrirá cuando el dispositivo en el que se detectó la amenaza se quitó recientemente de Intune.	El problema se resolverá en un plazo de 48 horas. No se requieren pasos adicionales.

Líneas base

Expandir tabla

Problema	Descripción	Solución
Configuración en conflicto al comparar la autenticación heredada de bloque y los pasos de implementación de MFA	Si un inquilino de cliente ha implementado la autenticación heredada de bloque y uno de los pasos de implementación de MFA, una prueba de comparación describirá erróneamente esta configuración como en conflicto.	No se requiere ninguna solución alternativa. La configuración no entra en conflicto y los usuarios del inquilino del cliente no se ven afectados.

Windows 365

Expandir tabla

Problema	Descripción	Solución
Error de aprovisionamiento de reintentos	Los técnicos de MSP reciben un mensaje de error "No tiene permisos para hacerlo" al intentar reintentar el aprovisionamiento de un equipo en la nube.	Para solucionar este problema, inicie sesión en el inquilino del cliente y, a continuación, vuelva a aprovisionar equipos en la nube desde el Centro de administración de Microsoft Endpoint Manger. Para obtener instrucciones, consulte Reprovision a Cloud PC(Reprovision a Cloud PC).

Privilegios administrativos delegados (DAP)

Expandir tabla

Problema	Descripción	Solución
Retraso de permisos al cambiar los roles de DAP	Si se agrega o quita un técnico de MSP del grupo agente de Administración o agente del departamento de soporte técnico, puede haber un retraso en la reflexión de los permisos adecuados en Lighthouse.	El problema se resolverá en un plazo de 30 minutos. No se requieren pasos adicionales.

Privilegios administrativos delegados granulares (GDAP)

Se requieren privilegios administrativos delegados granulares (GDAP) más una relación de revendedor indirecto o una relación de privilegios administrativos delegados (DAP) para incorporar clientes a Lighthouse. Si DAP y GDAP coexisten en un inquilino de cliente, los permisos de GDAP tienen prioridad para los técnicos de MSP en grupos de seguridad habilitados para GDAP. Los clientes con relaciones solo de GDAP (sin relaciones de revendedor indirecto) actualmente no pueden incorporarse a Lighthouse, pero podrán incorporarse en una versión futura.

Expandir tabla

Problema	Descripción	Solución
Varios problemas de permisos de GDAP en Lighthouse	Determinados roles de GDAP por sí mismos no conceden el mismo nivel de acceso a los datos del cliente en Lighthouse que en una experiencia de inquilino único. Si alguno de los siguientes roles se asigna individualmente (es decir, no en combinación con otros roles de GDAP) a los técnicos de MSP, pueden encontrar errores, incluidos: • Los administradores de seguridad de GDAP no pueden ver usuarios de riesgo, descartar riesgos o confirmar usuarios en peligro en Lighthouse. • Los lectores de seguridad de GDAP no pueden ver usuarios de riesgo en Lighthouse. • Los administradores globales de GDAP ven un mensaje de error al intentar ver el estado del servicio en Lighthouse. • Los administradores globales de GDAP experimentan problemas al implementar los pasos del plan de implementación en Lighthouse.	La solución alternativa consiste en asignar una combinación de roles GDAP a los técnicos de MSP en función del nivel de acceso a los datos del cliente que necesitan. Para obtener una lista de los roles de GDAP recomendados para usar Lighthouse, consulte Introducción a los permisos en Microsoft 365 Lighthouse. Para los problemas en los que incluso los permisos de administrador global de GDAP no permiten el uso de una característica en Lighthouse, la solución alternativa es acceder al centro de administración adecuado desde el inquilino del cliente para administrar al cliente (por ejemplo, acceder a la Centro de administración de Microsoft 365 desde el inquilino del cliente para comprobar el estado del servicio). Para obtener instrucciones sobre cómo modificar una relación GDAP, consulte Obtención de permisos de administrador pormenorizados para administrar el servicio de un cliente: Centro de partners.

Localización

Expandir tabla

Problema	Descripción	Solución
Problemas de traducción	Los usuarios pueden experimentar problemas de traducción de idioma cuando el idioma de su explorador, o su selección de idioma en Lighthouse, no sea inglés.	Para minimizar los problemas de traducción en Lighthouse, asegúrese de que la selección de idioma del explorador coincide con la de la configuración de idioma en el portal de Lighthouse. Para cambiar la selección de idioma en Lighthouse, inicie sesión en Lighthouse y seleccione el icono de engranaje de la parte superior de la página para abrir la página Configuración del portal, seleccione **Idioma y región** y, a continuación, seleccione el idioma y los formatos regionales adecuados.

Asesor de ventas

Expandir tabla

Problema	Descripción	Solución
Falta de coincidencia entre el número total de inquilinos y el número total de puestos con el Centro de partners	El número total de puestos e inquilinos que se muestran en la vista de resumen de las pestañas Adquisición de clientes, Retención de clientes y Crecimiento del cliente no coinciden entre la experiencia de Lighthouse y la experiencia del Centro de partners.	No se requiere ninguna solución alternativa. Este problema no afecta al número de oportunidades visibles en la tabla de recomendaciones o en la exportación. Todavía tiene acceso a la lista completa de oportunidades disponibles en los inquilinos del cliente.
La experiencia de filtrado y ordenación en Lighthouse es diferente de la del Centro de partners	La ordenación de columnas, el filtro recomendación, el filtro producto y el filtro de id. de MPN no están disponibles en la experiencia de Lighthouse.	No se requiere ninguna solución alternativa. Todavía tiene acceso a la lista completa de oportunidades disponibles en los inquilinos del cliente.

Contenido relacionado

Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)
Solución de problemas y mensajes de error en Microsoft 365 Lighthouse (artículo)
Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Solución de problemas y mensajes de error en Microsoft 365 Lighthouse

Artículo • 20/01/2025

En este artículo se describen los mensajes de error y los problemas que puede encontrar al usar Microsoft 365 Lighthouse y se proporcionan los pasos de solución de problemas que puede seguir para resolverlos.

Incorporación de asociados

Mensaje al intentar acceder a Lighthouse: "Microsoft 365 Lighthouse no admite proveedores indirectos en este momento, debe ser revendedor indirecto o asociado de factura directa para usar este servicio".

Causa: Intentó acceder a Lighthouse como asociado de factura indirecta. En este momento, Lighthouse solo admite revendedores indirectos y asociados de factura directa.

Resolución: Para obtener una lista completa de calificaciones y requisitos, consulte Requisitos para Microsoft 365 Lighthouse. Si no es un proveedor indirecto y cree que ha recibido este mensaje por error, póngase en contacto con el soporte técnico. Para obtener más información, consulte Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse.

Mensaje al intentar acceder a Lighthouse: "Debe ser revendedor indirecto o asociado de factura directa para usar este servicio".

Causa: Intentó acceder a Lighthouse y no es un partner de Microsoft. Debe estar inscrito en el programa Proveedor de soluciones en la nube (CSP) como revendedor indirecto o asociado de factura directa para usar Lighthouse.

Resolución: Para obtener una lista completa de calificaciones y requisitos, consulte Requisitos para Microsoft 365 Lighthouse. Si cumple los requisitos para acceder a Lighthouse y cree que ha recibido este mensaje por error, póngase en contacto con el soporte técnico. Para obtener más información, consulte Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse.

Mensaje al iniciar sesión en Lighthouse: "Microsoft 365 Lighthouse se quitó para su organización"

Causa: Microsoft 365 Lighthouse está deshabilitado en el inquilino del asociado.

Resolución: Para permitir el uso de Microsoft 365 Lighthouse, póngase en contacto con un administrador del inquilino del asociado y pídale que siga estos pasos:

1. Vaya a la Centro de administración de Microsoft 365 en https://admin.microsoft.com e inicie sesión con sus credenciales de inquilino de asociado.
2. En el panel de navegación izquierdo, seleccione **Configuración Configuración>de la organización**.
3. En la pestaña **Servicios**, seleccione **Microsoft 365 Lighthouse** en la lista de servicios y, a continuación, seleccione la opción para permitir el uso de Microsoft 365 Lighthouse experiencias de administración de clientes en el inquilino.
4. Haga clic en **Guardar**.

Incorporación de inquilinos del cliente

Los inquilinos del cliente muestran un estado distinto de "Administrado" en la lista de inquilinos

Causa: Los inquilinos del cliente no cumplen los siguientes criterios:

- Debe tener el acceso delegado configurado para que el proveedor de servicios administrados (MSP) pueda administrar el inquilino del cliente*
- Debe tener al menos una suscripción Enterprise, Business, Frontline o Education de Microsoft 365, Office 365, Exchange Online, Windows 365 Business o Microsoft Defender para Empresas
- No debe tener más de 2500 usuarios con licencia
- Debe residir en la misma región geográfica (América, Unión Europea o Asia más Australia) que la organización asociada que los administra.

Resolución: En la tabla siguiente se describen los distintos estados de inquilino que requieren acción y se explica cómo resolverlos.

Se requieren privilegios administrativos delegados granulares (GDAP) más una relación de revendedor indirecto o una relación de privilegios administrativos delegados (DAP)

para incorporar clientes a Lighthouse. Si DAP y GDAP coexisten en un inquilino de cliente, los permisos de GDAP tienen prioridad para los técnicos de MSP en grupos de seguridad habilitados para GDAP. Próximamente, los clientes con relaciones solo de GDAP (sin relaciones de revendedor indirecto) podrán incorporarse a Lighthouse.

Expandir tabla

Estado	Descripción	Solución
Limitado	Este inquilino de cliente solo tiene acceso a un conjunto limitado de experiencias en Lighthouse, incluida la configuración y administración de GDAP, la búsqueda de usuarios, los detalles del usuario, el etiquetado de inquilinos y el estado del servicio.	Seleccione el nombre del inquilino para ver un estado detallado de los requisitos de administración de Lighthouse. Para obtener más información, consulte Requisitos para Microsoft 365 Lighthouse.
Quitado por asociado	Su organización ha excluido a este inquilino de cliente de la administración de Lighthouse.	Debe reactivar el inquilino para su administración mediante Lighthouse. En la página **Inquilinos** , seleccione los tres puntos (más acciones) junto al inquilino que desea administrar y, a continuación, seleccione **Administrar inquilino**. Los datos iniciales del cliente pueden tardar entre 24 y 48 horas en aparecer en Lighthouse.
Quitado por el cliente	El cliente decidió no permitir el uso de Microsoft 365 Lighthouse para administrar su inquilino.	Un administrador del inquilino del cliente debe ir a Configuración de la **organización** en el Centro de administración de Microsoft 365, seleccionar **Microsoft 365 Lighthouse** en la pestaña **Servicios** y, a continuación, seleccionar la opción para permitir el uso de Microsoft 365 Lighthouse experiencias de administración de clientes en su inquilino.
Error	Se produjo un error durante el proceso de incorporación de este inquilino de cliente y estamos trabajando en una corrección.	Si este error persiste durante más de 48 horas, póngase en contacto con el soporte técnico.

Si ha confirmado que el inquilino del cliente cumple los criterios de incorporación y que todavía no se muestran como **Administrado** en Lighthouse, póngase en contacto con el soporte técnico. Para obtener más información, consulte Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse.

Acceso y permisos

Mensaje al intentar acceder a Lighthouse: "No autorizado" o "Privilegios insuficientes" o "Restricción de acceso: Insuficiente o falta de permisos está causando restricción de acceso"

Causa: No pertenece al grupo de seguridad correcto en Microsoft Entra ID o no se le ha asignado el rol correcto en el Centro de partners para poder acceder a Lighthouse.

Resolución: Asegúrese de que un administrador del inquilino del asociado le asignó al grupo de seguridad de GDAP correcto en Microsoft Entra ID y le asignó el rol correcto en el Centro de partners. Además, tenga en cuenta que algunas acciones de Lighthouse requieren que tenga el rol de administrador en Lighthouse. Para más información sobre los roles de GDAP y lo que puede hacer cada rol, consulte Introducción a los permisos en Microsoft 365 Lighthouse. Para obtener una descripción detallada de todos los Microsoft Entra roles y permisos integrados para GDAP, consulte Microsoft Entra roles integrados.

En el caso de los clientes con relaciones de DAP, el administrador del asociado deberá asignarle el rol de agente de Administración o agente del departamento de soporte técnico en el Centro de partners. Para obtener una descripción detallada de todos los roles y permisos del Centro de partners, consulte Asignación de roles y permisos a usuarios: Centro de partners.

No veo datos completos en ciertas áreas de Lighthouse, o no puedo realizar ciertas tareas, o no puedo acceder a determinados inquilinos.

Causa: Tiene acceso GDAP limitado en función de los roles asignados al grupo de seguridad Microsoft Entra en el que se encuentra.

Resolución: Asegúrese de que un administrador del inquilino del asociado le asignó al grupo de seguridad de GDAP correcto en Microsoft Entra ID. Además, tenga en cuenta que algunas acciones de Lighthouse requieren que tenga el rol de administrador en Lighthouse. Para más información sobre los roles de GDAP y lo que puede hacer cada rol, consulte Introducción a los permisos en Microsoft 365 Lighthouse. Para obtener una descripción detallada de todos los Microsoft Entra roles y permisos integrados para GDAP, consulte Microsoft Entra roles integrados.

Configuración y administración de GDAP

Mensaje al ejecutar el programa de instalación de GDAP: "No se pudo crear una relación"

Causa: No tiene los roles necesarios para configurar GDAP en Lighthouse, o la configuración en los inquilinos de asociados o clientes impide que complete la configuración de GDAP.

Resolución: Asegúrese de que tiene los roles necesarios para ejecutar el programa de instalación de GDAP, incluido el administrador (asignado en Lighthouse) y Administración agente (asignado en el Centro de partners). Además, asegúrese de que su cuenta cumple los requisitos de seguridad para ejecutar el programa de instalación de GDAP, incluido asegurarse de que no es un usuario de riesgo y de que tiene la autenticación multifactor (MFA) configurada. Para comprobar y corregir los riesgos de su cuenta, consulte Corrección de riesgos y desbloqueo de usuarios. Para obtener instrucciones sobre cómo exigir MFA, consulte Mandating MFA for your partner tenant - Partner Center (Creación de MFA para el inquilino del asociado: Centro de partners).

También debe asegurarse de que las directivas de acceso condicional configuradas en los inquilinos del cliente no bloqueen la capacidad de establecer una relación GDAP con ellos. Para obtener instrucciones paso a paso sobre cómo confirmar esto, consulte ¿Cuál es el paso siguiente recomendado si la directiva de acceso condicional establecida por el cliente bloquea todo el acceso externo?.

Los grupos de seguridad no se asignan a las relaciones de GDAP después de ejecutar la instalación de GDAP

Causa: No ha completado todos los pasos del programa de instalación de GDAP o la relación GDAP creada por el programa de instalación de GDAP todavía requiere la aprobación del cliente.

Resolución: Debe completar cada paso del programa de instalación de GDAP para que se apliquen todas las configuraciones y asegúrese de seleccionar **Finalizar** cuando haya terminado. En la última página del programa de instalación de GDAP, los clientes con un estado *Activo* tendrán asignados grupos de seguridad. Si no tiene consentimiento para administrar servicios para ninguno de sus clientes, deberá enviarles una solicitud de relación de administrador. Una vez que aprueben la solicitud, vuelva a ejecutar el programa de instalación de GDAP para asignar los grupos de seguridad a la relación GDAP creada para esos clientes.

Faltan algunos usuarios del inquilino de mi asociado al configurar alertas o asignar usuarios a grupos de seguridad en el programa de instalación de GDAP.

Causa: El campo **Tipo de usuario** de la cuenta de Microsoft Entra ID está en blanco o está establecido en *Invitado*.

Resolución: Asegúrese de que un administrador del inquilino del asociado ha establecido **Tipo de usuario** en *Miembro* en la cuenta de Microsoft Entra ID.

Administración de inquilinos del cliente

El inquilino del cliente no tiene datos que se muestren en Lighthouse

Causa: Está intentando ver los datos en Lighthouse antes de que se complete la incorporación de inquilinos.

Resolución: Los datos iniciales del cliente pueden tardar entre 24 y 48 horas en aparecer en Lighthouse. Si han pasado más de 48 horas desde que incorporó el inquilino y aún no puede ver ni cargar datos del inquilino, o no puede ver ni cargar los datos que anteriormente había podido, póngase en contacto con el soporte técnico. Para obtener más información, consulte Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse. Esté preparado para proporcionar los registros de red pertinentes y una lista de las opciones que se hayan modificado.

Los datos del inquilino del cliente no se actualizan después de realizar cambios en el inquilino del cliente

Causa: Los cambios realizados dentro del inquilino del cliente pueden tardar hasta 4 horas en sincronizarse con los datos del inquilino del cliente en Lighthouse.

Resolución: Si han pasado más de 4 horas y los datos del inquilino del cliente siguen sin actualizarse en Lighthouse, póngase en contacto con el soporte técnico. Para obtener más información, consulte Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse. Prepárese para proporcionar información sobre el inquilino del cliente.

Mensaje al aplicar una línea base a un inquilino de cliente: "Error de proceso"

Causa: No ha completado correctamente la configuración de Microsoft Intune dentro del inquilino del cliente.

Resolución: Compruebe que ha completado los pasos de configuración básicos para Intune dentro del inquilino del cliente. Si el problema persiste después de comprobar que Intune configuración está completa para el inquilino del cliente, póngase en contacto con el soporte técnico. Para obtener más información, consulte Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse.

No se puede acceder a los datos del inquilino del asociado en Lighthouse

Causa: Lighthouse solo admite la visualización y administración de inquilinos de *clientes* . Actualmente no admite la visualización y *administración de* inquilinos asociados.

Resolución: Siga usando cualquier método que haya usado para ver y administrar el inquilino del asociado.

Administración de dispositivos y amenazas

No veo ningún dato de inquilino de cliente en las páginas Cumplimiento de dispositivos y Administración de amenazas de Lighthouse

Causa 1: El inquilino del cliente no ha completado la incorporación a Intune. Los datos del inquilino del cliente no estarán disponibles en las páginas Cumplimiento de dispositivos o Administración de amenazas de Lighthouse hasta que el inquilino del cliente haya completado la incorporación a Intune.

Resolución: Compruebe que el inquilino del cliente para el que intenta ver los datos ha completado la incorporación a Intune. Una vez completada la incorporación en Intune, espere 4 horas para que los datos del dispositivo aparezcan en Lighthouse.

Causa 2: El inquilino del cliente se ha incorporado recientemente a Lighthouse y los datos se siguen cargando en Lighthouse.

Resolución: Una vez que un inquilino de cliente se incorpore a Lighthouse, permita que aparezcan entre 24 y 48 horas para que aparezcan los datos iniciales del cliente.

Causa 3: El dispositivo de inquilino del cliente es nuevo y los datos del dispositivo se siguen cargando en Lighthouse.

Resolución: Cuando se agrega un dispositivo de inquilino, espere 4 horas para que los datos del dispositivo aparezcan en Lighthouse.

Si los datos siguen sin aparecer en las páginas Cumplimiento de dispositivos y Administración de amenazas después de seguir las instrucciones de resolución, póngase en contacto con el soporte técnico. Para obtener más información, consulte Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse.

Asesor de ventas

Mensaje al ver la página Oportunidades de Sales Advisor en Lighthouse: "No tiene permiso para ver la información de esta página"

Causa: No tiene los permisos correctos en el Centro de partners para ver las páginas de Sales Advisor en Lighthouse.

Resolución: Compruebe que tiene el rol Administrador de cuentas en Lighthouse. Si no tiene el rol Administrador de cuentas, póngase en contacto con alguien que tenga el rol Administrador en Lighthouse y pídale que le asigne el rol. Para obtener más información, consulte Obtener acceso a Sales Advisor en Microsoft 365 Lighthouse.

Mensaje al ver la página Oportunidades de Sales Advisor en Lighthouse: "No hay oportunidades"

Causa 1: Es posible que el modelo de propensión de Sales Advisor no genere nuevas recomendaciones para los clientes. Esto significa que actualmente no hay oportunidades para ver o actuar.

Resolución: Vuelva a comprobar en dos semanas para ver si se han generado nuevas recomendaciones.

Causa 2: Hay un problema técnico en nuestro back-end que impide que se muestren oportunidades.

Resolución: Abra una solicitud de servicio siguiendo las instrucciones de Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse. Para crear una solicitud de servicio de Lighthouse, asegúrese de que tiene asignado un rol de inquilino de asociado y al menos un rol de Microsoft Entra con el siguiente conjunto de propiedades: **microsoft.office365.supportTickets/allEntities/allTasks**. Para obtener una lista completa de Microsoft Entra roles, consulte Microsoft Entra roles integrados.

Mensaje al intentar acceder a Lighthouse desde la pestaña Partner Insights del Asesor de ventas: "Debe ser un revendedor indirecto o asociado de factura directa para usar este servicio" o se me redirige a la página principal de Lighthouse, pero no puede iniciar sesión.

Causa 1: Microsoft 365 Lighthouse aún no se ha implementado en el inquilino del asociado.

Resolución: Trabaje con alguien que tenga el rol de administrador en Lighthouse para implementar Lighthouse en el inquilino del asociado. Para obtener más información, vea Registrarse para Microsoft 365 Lighthouse.

Causa 2: Su organización tiene varios inquilinos de asociados y ha intentado acceder a Lighthouse con las credenciales de un inquilino asociado que aún no ha implementado Lighthouse.

Resolución: Use las mismas credenciales de Microsoft Entra que usó para iniciar sesión en el Centro de partners para acceder a Lighthouse. Si no está seguro, póngase en contacto con alguien del inquilino del asociado que tenga los permisos adecuados para confirmar qué inquilinos de asociados han implementado Lighthouse. Si es necesario, pídales que implementen Lighthouse en el inquilino del asociado que intenta usar. Para obtener más información, vea Registrarse para Microsoft 365 Lighthouse.

Causa 3: Intentó acceder a Lighthouse desde un inquilino asociado que no está calificado para usar Lighthouse. En este momento, Lighthouse solo admite revendedores indirectos y asociados de factura directa.

Resolución: Para obtener una lista completa de calificaciones y requisitos, consulte Requisitos para Microsoft 365 Lighthouse. Si no es un proveedor indirecto y cree que ha recibido este mensaje por error, póngase en contacto con el soporte técnico. Para obtener más información, consulte Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse.

Los datos o oportunidades que se muestran en las páginas de Sales Advisor parecen inexactos

Causa: Si ve una oportunidad con un cliente que no reconoce, es posible que tenga información incompleta o incorrecta sobre la relación de asociado que su organización tiene con ese cliente.

Resolución: Abra una solicitud de servicio siguiendo las instrucciones de Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse. Para crear una solicitud de servicio de Lighthouse, asegúrese de que tiene asignado un rol de inquilino de asociado y al menos un rol de Microsoft Entra con el siguiente conjunto de propiedades: **microsoft.office365.supportTickets/allEntities/allTasks**. Para obtener una lista completa de Microsoft Entra roles, consulte Microsoft Entra roles integrados.

Contenido relacionado

Problemas conocidos con Microsoft 365 Lighthouse (artículo)
Preguntas más frecuentes sobre Microsoft 365 Lighthouse (artículo)
Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse (artículo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Microsoft 365 Lighthouse preguntas más frecuentes (P+F)

Preguntas más frecuentes

Última actualización del 27 de agosto de 2024. Este artículo contiene respuestas a las preguntas más frecuentes sobre Microsoft 365 Lighthouse.

Si no encuentra una respuesta a su pregunta, háganoslo saber proporcionando comentarios y lo agregaremos a este artículo.

Introducción

¿Qué es Microsoft 365 Lighthouse?

Microsoft 365 Lighthouse ayuda a los proveedores de servicios administrados (MSP) a aumentar su negocio y a ofrecer servicios a los clientes a escala a través de la administración proactiva de cuentas, la incorporación simplificada, la configuración eficaz del inquilino, la protección de dispositivos y las alertas. Lighthouse proporciona información sobre las oportunidades de adquisición, retención y crecimiento del cliente, así como vistas multiinquilino entre dispositivos de clientes, datos y usuarios para ayudarle a anticipar las necesidades de los clientes y maximizar su inversión en Microsoft 365.

Para los técnicos de servicio de MSP con acceso delegado, Lighthouse le ayuda a proteger y administrar dispositivos, datos y usuarios a escala para clientes de pequeñas y medianas empresas (SMB). Lighthouse simplifica la incorporación de inquilinos mediante la recomendación de líneas base de configuración de seguridad adaptadas a las PYME y que proporcionan vistas multiinquilino en todos los entornos de cliente.

Para los administradores de cuentas, los profesionales de ventas y los usuarios de éxito del cliente, la funcionalidad de Sales Advisor en Lighthouse usa inteligencia artificial (IA) para analizar la base de clientes y aplicar modelos de datos (creados por científicos de datos de Microsoft) para identificar oportunidades en las que puede interactuar, nutrir y aumentar el uso de Microsoft 365 de su cliente a través de recomendaciones accionables e instrucciones prescriptivas.

Para obtener más información, vea Información general de Microsoft 365 Lighthouse.

¿Cuánto cuesta Microsoft 365 Lighthouse?

No hay costos adicionales asociados con el uso de Lighthouse para administrar varios inquilinos de clientes de Microsoft 365. Lighthouse está disponible para los MSP que atienden pequeñas y medianas empresas y que tienen una relación de proveedor de soluciones en la nube (CSP) con sus clientes. Para obtener más información, consulte Requisitos para Microsoft 365 Lighthouse.

¿Cuáles son los requisitos para usar Microsoft 365 Lighthouse?

Para obtener una lista de los requisitos actuales, consulte Requisitos para Microsoft 365 Lighthouse.

¿En qué países y regiones está disponible Microsoft 365 Lighthouse?

Lighthouse está disponible en todos los países donde Microsoft 365 está disponible, excepto China y la Autoridad Palestina. Sin embargo, las características de Lighthouse, como la administración de dispositivos y la administración de amenazas, se basan en Microsoft Intune y la administración de usuarios se basa en Microsoft Entra ID, y es posible que Intune y Microsoft Entra ID no estén disponibles en determinados países y regiones. Para obtener una lista completa de la disponibilidad de Microsoft 365, Microsoft Entra ID y Intune, consulte Disponibilidad internacional.

Lighthouse no está disponible en nubes nacionales.

Cómo registrarse para Microsoft 365 Lighthouse?

Para registrarse en Lighthouse, deberá inscribirse en el programa Proveedor de soluciones en la nube (CSP) como revendedor indirecto o asociado de factura directa. Para obtener instrucciones sobre cómo registrarse, consulte Registrarse para Microsoft 365 Lighthouse. Para obtener más información sobre el programa CSP, consulte introducción al programa Proveedor de soluciones en la nube: Centro de partners.

¿Microsoft 365 Lighthouse funcionará si los inquilinos de mis clientes tienen una combinación de suscripciones?

Sí, pero las funcionalidades de Lighthouse variarán en función de las licencias asignadas al usuario. Por ejemplo, si a un usuario le falta una licencia que incluye Intune, los dispositivos de ese usuario, el estado de cumplimiento del dispositivo y el estado de amenazas no estarán disponibles; y si falta una licencia que incluya Microsoft Entra ID P1, la administración de contraseñas e inicios de sesión de ese usuario no estará disponible. Para obtener más información, consulte Requisitos para Microsoft 365 Lighthouse.

Administración de inquilinos de clientes

He terminado de registrarme, ¿por qué no veo los datos del inquilino del cliente?

Los datos del inquilino del cliente pueden tardar hasta 48 horas en cargarse en Lighthouse. Si han pasado más de 48 horas desde que completó la incorporación, póngase en contacto con nuestro equipo de soporte técnico para obtener ayuda. Deberá informarles cuando haya completado la incorporación y proporcionar las capturas de pantalla y los registros pertinentes. Para obtener más información, consulte Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse.

¿Por qué veo datos de algunos inquilinos de clientes, pero no de otros?

Para que los datos del inquilino del cliente aparezcan en Lighthouse, los CSP deben establecer el acceso delegado para administrar el inquilino del cliente. Se requieren privilegios administrativos delegados granulares (GDAP) más una relación de revendedor indirecto o una relación de privilegios administrativos delegados (DAP) para incorporar clientes a Lighthouse. Se recomienda establecer GDAP con los clientes para permitir un acceso delegado más seguro. Si DAP y GDAP coexisten en un inquilino de cliente, los permisos de GDAP tienen prioridad para los técnicos de MSP en grupos de seguridad habilitados para GDAP. Para obtener más información sobre el acceso delegado, consulte Solicitud de una relación de revendedor con un cliente en el Centro de partners. Los inquilinos también deben tener al menos una suscripción Enterprise, Business, Frontline o Education de Microsoft 365, Office 365, Exchange Online, Windows 365 Business o Microsoft Defender para Empresas y no más de 2500 usuarios con licencia en su inquilino. Para obtener más información, consulte la página Requisitos para Microsoft 365 Lighthouse e Información general de los inquilinos en Microsoft 365 Lighthouse.

Si GDAP se establece con el cliente, un técnico de MSP debe estar en un grupo de seguridad habilitado para GDAP que tenga asignados los roles adecuados para poder administrar los datos de ese cliente en Lighthouse. Los roles de GDAP asignados a ese grupo de seguridad afectan a qué datos de cliente se pueden administrar en Lighthouse. Consulte Introducción a los permisos en Microsoft 365 Lighthouse para obtener más información sobre qué roles de inquilino delegados y asociados se recomiendan para usar Lighthouse. Para obtener instrucciones sobre cómo ver qué roles de GDAP se le han asignado para diferentes inquilinos de clientes en Lighthouse, consulte Visualización de los roles de Microsoft Entra en Microsoft 365 Lighthouse.

¿Qué ocurre si no quiero ver ciertos inquilinos en Microsoft 365 Lighthouse?

Si no desea ver determinados inquilinos y sus datos en Lighthouse, puede quitar esos inquilinos. Para quitar un inquilino, siga estos pasos:

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos** para abrir la página **Inquilinos** .
2. Busque el inquilino que desea quitar, seleccione los tres puntos (más acciones) junto al nombre del inquilino y, a continuación, seleccione **Quitar inquilino**.
3. En el cuadro de diálogo de confirmación, seleccione **Confirmar** para quitar el inquilino.

> **Nota**
>
> Una vez que quite un inquilino, no podrá realizar ninguna acción en el inquilino hasta que se complete el proceso de eliminación. Este proceso puede tardar hasta 48 horas en completarse.

Para obtener más información sobre los inquilinos, consulte introducción a la página Microsoft 365 Lighthouse inquilinos.

¿Qué permisos tengo actualmente para este inquilino?

Si no puede acceder a la información del inquilino, es posible que no tenga los permisos correctos para ese inquilino. Algunas características y datos solo son visibles para roles específicos. Para ver qué roles tiene, consulte Visualización de los roles de Microsoft Entra entre inquilinos.

¿Puedo usar Microsoft 365 Lighthouse para administrar el inquilino de mi asociado?

No, solo puede usar Lighthouse para administrar los inquilinos de clientes con los que tiene una relación de revendedor o GDAP.

Descripción de las alertas

¿Por qué hay comentarios que no he agregado en mis alertas?

Lighthouse agrega comentarios cada vez que el sistema realiza un cambio o actualiza una alerta. Del mismo modo, si un usuario realiza una acción en una alerta, esto también se anota en un comentario. Estos comentarios proporcionan un historial en ejecución de todas las acciones realizadas en la alerta.

He resuelto una alerta en el portal de servicios asociado. ¿Por qué sigo viendo la alerta en Lighthouse?

Las alertas de Lighthouse se basan en la entidad subyacente (por ejemplo, el dispositivo o el usuario) y no se correlacionan con las alertas del portal de servicios asociado. Si resuelve una alerta en el portal de servicios asociado pero no realiza un cambio en la entidad subyacente, la alerta de Lighthouse permanece sin cambios. Si realiza un cambio en la entidad subyacente, el estado de la alerta de Lighthouse cambia a **Resuelto**.

¿Por qué las alertas se muestran de nuevo después de que se descartan o se resuelven?

Si se resuelve una alerta pero vuelve a aparecer el problema subyacente, la alerta se desencadena de nuevo y el estado cambia a **Nuevo**. Por ejemplo, si se resuelve una alerta de usuario de riesgo, pero el mismo usuario de riesgo desencadena una nueva alerta con un nuevo comportamiento de riesgo, el estado de la alerta cambia de **Resuelto** a **Nuevo**.

Cuando se descarta una alerta en Lighthouse, la entidad desencadenante (por ejemplo, usuario o dispositivo) no volverá a intentar la misma alerta durante 30 días. Después de

30 días, cualquier actividad nueva en esa entidad cambia el estado de alerta de **Descartado** a **Nuevo**.

¿Cuándo se envían los correos electrónicos de notificación de alertas?

Lighthouse supervisa todos los portales de servicio correspondientes entre los MSP y sus clientes. La hora exacta en que aparece una alerta y se envía un correo electrónico de notificación varía y se basa en el motor de reglas de alertas, pero los MSP normalmente deberían ver una nueva alerta en la página **Alertas** de Lighthouse y recibir una notificación por correo electrónico en cuestión de minutos después del evento desencadenante.

¿Qué indican las marcas de tiempo en las alertas de Lighthouse?

La marca de tiempo de la columna **Primera detectada** indica la primera vez que Lighthouse detectó el problema. Esta marca de tiempo puede ser ligeramente diferente de la marca de tiempo de la alerta en el portal de servicios asociado.

La marca de tiempo de la columna **Última actualización** indica la hora en que Lighthouse detectó por última vez el problema.

Implementación de líneas base

¿Qué ocurre si tengo un inquilino de cliente que usa una solución antivirus de terceros y no quiero configurar Microsoft Defender para Empresas?

En el plan de implementación del inquilino del cliente, en la tarea **Configurar Microsoft Defender para Empresas** implementación, descarte la subtarea **Aprovisionamiento** y seleccione **Resuelto a través de un tercero** como motivo del despido.

¿Qué ocurre si no quiero requerir MFA para una cuenta de administrador de acceso de emergencia?

Realiza una de las siguientes acciones:

- Excluya la cuenta de administrador de acceso de emergencia de la tarea de implementación **Requerir MFA para administradores** .

    1. En el plan de implementación del inquilino del cliente asociado a la cuenta de administrador de acceso de emergencia, en la tarea de implementación **Requerir MFA para administradores** , seleccione la subtarea **Crear directiva de acceso condicional para requerir MFA para administradores** para abrir el panel de detalles de la tarea y, a continuación, seleccione **Implementar**.
    2. En la página **Revisar tarea de implementación** , haga clic en el campo **Excluir usuarios** para abrir la lista de usuarios sugeridos y, a continuación, seleccione la cuenta de administrador de acceso de emergencia que desea excluir.
    3. Seleccione **Siguiente** para revisar las configuraciones detectadas y, a continuación, continúe con la confirmación e implementación.

- En el plan de implementación del inquilino del cliente asociado a la cuenta de administrador de acceso de emergencia, en la tarea de implementación **Requerir MFA para administradores** , descarte la subtarea **Crear directiva de acceso condicional para requerir MFA para administradores** y seleccione **Riesgo aceptado** como motivo del despido.

    > ⓘ **Nota**
    >
    > El despido de una tarea de implementación afecta a todos los usuarios del inquilino.

Cómo cambiar el estado de implementación de una configuración de "Solo informe" a "Habilitado" para una directiva de acceso condicional implementada a través de Lighthouse?

Realiza una de las siguientes acciones:

- Cambie el estado de implementación de la configuración existente a **Habilitado**.

    1. En el plan de implementación del inquilino del cliente, seleccione la subtarea correspondiente para abrir el panel de detalles de la tarea y, a continuación, seleccione **Historial de detección**.

2. Seleccione el examen más reciente del inquilino para ver la configuración del inquilino.
3. Seleccione la configuración para la que desea actualizar el estado de implementación para abrir la configuración en Microsoft Entra ID.
4. Cambie **Habilitar directiva** a **Activado** y, a continuación, seleccione **Guardar**.
5. Vuelva al panel de detalles de la tarea en Lighthouse y, a continuación, seleccione **Ejecutar detección** para actualizar el estado de implementación.

- Elimine la configuración existente y, a continuación, implemente una nueva configuración.

    1. En el plan de implementación del inquilino del cliente, seleccione la subtarea correspondiente para abrir el panel de detalles de la tarea y, a continuación, seleccione **Implementar**.
    2. Seleccione **Siguiente** para continuar con la página **Revisar configuraciones detectadas** .
    3. En la lista de configuraciones detectadas, seleccione la configuración aplicable para abrirla en Microsoft Entra ID.
    4. Elimine la configuración en Microsoft Entra ID.
    5. Vuelva a la página **Revisar configuraciones detectadas** en Lighthouse y, a continuación, seleccione **Actualizar** para actualizar las configuraciones detectadas.
    6. Seleccione **Siguiente** para confirmar e implementar.

Cómo corregir una configuración existente que tenga una configuración que no sea compatible con el plan de implementación?

Realiza una de las siguientes acciones:

- Edite la configuración dentro de la configuración existente para que sea compatible.

    1. En el plan de implementación del inquilino del cliente, seleccione la subtarea correspondiente para abrir el panel de detalles de la tarea y, a continuación, seleccione **Implementar**.
    2. Seleccione **Siguiente** para continuar con la página **Revisar configuraciones detectadas** .
    3. Seleccione la configuración que contiene la configuración que desea editar para abrirla en el portal de administración aplicable.

4. Edite la configuración, según sea necesario para la tarea y, a continuación, guarde la configuración actualizada.
5. En la página **Revisar configuraciones detectadas** de Lighthouse, seleccione **Actualizar** para actualizar las configuraciones detectadas. La tarea aplicable ahora debe mostrar un estado **compatible**.
6. Seleccione **Siguiente** para confirmar e implementar.

- Edite la asignación de la configuración existente para excluir a los usuarios que tienen asignada la tarea.

    1. En el plan de implementación del inquilino del cliente, seleccione la subtarea correspondiente para abrir el panel de detalles de la tarea y, a continuación, seleccione **Implementar**.
    2. En la página **Revisar configuraciones detectadas** , haga clic en el campo **Excluir usuarios** para abrir la lista de usuarios sugeridos y, a continuación, seleccione los usuarios que desea excluir.
    3. Seleccione **Siguiente** para revisar las configuraciones detectadas y, a continuación, continúe con la confirmación y la **implementación**.

- Elimine la configuración existente.

    1. En el plan de implementación del inquilino del cliente, seleccione la subtarea correspondiente para abrir el panel de detalles de la tarea y, a continuación, seleccione **Implementar**.
    2. Seleccione **Siguiente** para continuar con la página **Revisar configuraciones detectadas** .
    3. En la lista de configuraciones detectadas, seleccione la configuración aplicable para abrirla en Microsoft Entra ID.
    4. Elimine la configuración en Microsoft Entra ID.
    5. En la página **Revisar configuraciones detectadas** de Lighthouse, seleccione **Actualizar** para actualizar las configuraciones detectadas.
    6. Seleccione **Siguiente** para confirmar e implementar.

- Descarte la tarea asociada a la configuración que tiene una configuración no compatible.

    1. En el plan de implementación del inquilino del cliente, seleccione la tarea de implementación que desea descartar para abrir el panel de detalles de la tarea y, a continuación, seleccione **Descartar**.
    2. En **Motivo**, seleccione la opción adecuada y, a continuación, seleccione **Guardar**.

> ⓘ **Nota**
>
> El despido de una tarea de implementación afecta a todos los usuarios del inquilino.

¿Qué hago si hay usuarios que no tienen licencia para los servicios requeridos por la tarea de implementación?

Realiza una de las siguientes acciones:

- Excluya las cuentas de usuario aplicables de la tarea de implementación.

    1. En el plan de implementación del inquilino del cliente, seleccione la subtarea correspondiente para abrir el panel de detalles de la tarea y, a continuación, seleccione **Implementar**.
    2. En la página **Revisar tarea de implementación** , haga clic en el campo **Excluir usuarios** para abrir la lista de usuarios sugeridos y, a continuación, seleccione los usuarios que desea excluir.
    3. Seleccione **Siguiente** para revisar las configuraciones detectadas y, a continuación, continúe con la confirmación e implementación.

- Habilite la implementación mediante la asignación de licencias para los servicios necesarios a los usuarios aplicables.

    1. En el panel de navegación izquierdo de Lighthouse, seleccione**Administración de cuentas** de **usuarios**> y, a continuación, busque el usuario sin licencia.
    2. Seleccione el usuario adecuado para abrir el panel de detalles del usuario y, a continuación, seleccione **Licencias y aplicaciones**.
    3. Seleccione las licencias necesarias para la tarea de implementación y, a continuación, seleccione **Guardar cambios**.
    4. Repita estos pasos para cada usuario aplicable.

- Descarte la tarea para el inquilino del cliente.

    1. En el plan de implementación del inquilino del cliente, seleccione la tarea de implementación que desea descartar para abrir el panel de detalles de la tarea y, a continuación, seleccione **Descartar**.
    2. En **Motivo**, seleccione **Riesgo aceptado** y, a continuación, seleccione **Guardar**.

> ⓘ **Nota**
>
> El despido de una tarea de implementación afecta a todos los usuarios del inquilino.

Cómo excluir a un usuario invitado de una asignación de tareas?

Realiza una de las siguientes acciones:

- Excluya la cuenta de usuario aplicable de la tarea de implementación.

    1. En el plan de implementación del inquilino del cliente, seleccione la subtarea correspondiente para abrir el panel de detalles de la tarea y, a continuación, seleccione **Implementar**.
    2. En la página **Revisar tarea de implementación** , haga clic en el campo **Excluir usuarios** para abrir la lista de usuarios sugeridos y, a continuación, seleccione el usuario que desea excluir.
    3. Seleccione **Siguiente** para revisar las configuraciones detectadas y, a continuación, continúe con la confirmación e implementación.

- Excluya el grupo de seguridad aplicable de la tarea de implementación.

    1. En el plan de implementación del inquilino del cliente, seleccione la subtarea correspondiente para abrir el panel de detalles de la tarea y, a continuación, seleccione **Implementar**.
    2. En la página **Revisar tarea de implementación** , haga clic en el campo **Excluir grupos** para abrir la lista de grupos sugeridos y, a continuación, seleccione el grupo que desea excluir.
    3. Seleccione **Siguiente** para revisar las configuraciones detectadas y, a continuación, continúe con la confirmación e implementación.

¿Por qué una o varias tareas de implementación tienen el estado "No compatible"?

Las tareas **no son compatibles** si hay uno o varios usuarios para los que uno o más valores de configuración de la configuración asignada son **Falta** o **No compatible**.

Para investigar y resolver una tarea de implementación que **no es compatible**:

1. Abra el plan de implementación del inquilino del cliente y seleccione la tarea que desea investigar para abrir el panel de detalles de la tarea.

2. Seleccione **Progreso del usuario** para ver qué usuarios tienen el estado **No compatible** o **No con licencia**. Para resolver los usuarios que **no tienen licencia**, asígneles la licencia necesaria o excluya de la asignación de la tarea.

3. Si hay usuarios que **no son compatibles**, seleccione **Historial de detección** y, a continuación, seleccione el examen más reciente del inquilino para ver la configuración del inquilino.

   La configuración del inquilino identificará qué configuración dentro de la directiva para la que los usuarios son **faltantes** o **no compatibles**.

4. Realiza una de las siguientes acciones:

   - Para resolver los valores que **faltan**, agregue la configuración que falta a la configuración.
   - Para resolver la configuración que **no es compatible**, actualice el valor de la configuración aplicable para que coincida con el valor de la tarea de implementación y, a continuación, seleccione **Ejecutar detección** en el panel de detalles de la tarea.

¿Por qué uno o varios planes de implementación tienen el estado "No completado"?

Los planes de implementación **no están completos** si hay una o varias tareas que **no tienen licencia** o **no son compatibles**.

Para investigar y resolver un plan de implementación que **no está completo**:

1. Abra el plan de implementación del inquilino del cliente para ver el estado de las tareas de implementación asignadas.

2. Revise cada tarea de implementación que tenga el estado **No con licencia** o **No compatible** y, a continuación, realice una de las siguientes acciones:

   - Para resolver las tareas de implementación que **no tienen licencia**, asigne la licencia necesaria a cada uno de los usuarios de destino o descarte la tarea del plan de implementación.
   - Para resolver las tareas de implementación que **no son compatibles**, complete la implementación de la tarea o descarte la tarea del plan de implementación.

¿Por qué Lighthouse sigue notificando las licencias como necesarias cuando ya las he asignado a los usuarios necesarios en el Centro de administración de Microsoft 365?

Cuando se actualiza la configuración de un inquilino de cliente en Lighthouse, el estado de implementación del inquilino se actualiza automáticamente. Sin embargo, los cambios realizados fuera de Lighthouse no se detectan inmediatamente. Los cambios externos no se detectarán hasta el siguiente examen programado de Lighthouse o hasta que un usuario de Lighthouse inicie manualmente un examen de detección.

Por ejemplo, si Lighthouse indica que un usuario no tiene licencia para una tarea, puede resolverlo asignando la licencia necesaria al usuario en el Centro de administración de Microsoft 365. Después, realice una de las siguientes acciones para ver la asignación de licencia reflejada en el estado de implementación en Lighthouse:

- Inicie manualmente un examen seleccionando **Ejecutar detección** para la tarea de implementación. Esto actualiza inmediatamente el estado de implementación del usuario.
- Espere a que Lighthouse vuelva a examinar automáticamente el inquilino y actualice el estado de implementación.

Administración de equipos en la nube de Windows 365

Cómo calificar para administrar equipos en la nube del cliente en Microsoft 365 Lighthouse?

Si cumple los requisitos para usar Lighthouse, está cualificado para administrar equipos en la nube del cliente en Lighthouse. Para obtener una lista de los requisitos actuales, consulte Requisitos para Microsoft 365 Lighthouse.

¿Dónde puedo comprar licencias de Windows 365 (PC en la nube) para mis clientes?

Puede comprar licencias de Windows 365 a través de todos los canales de ventas comerciales de Microsoft disponibles. Una licencia comprada equivale a la compra de un equipo en la nube. Actualmente, a cada usuario solo se le puede asignar un equipo en la

nube del mismo tipo de SKU, pero se le pueden asignar varios equipos en la nube si son de tipos de SKU diferentes. Para comparar Windows 365 planes y precios, consulte Obtener el PC en la nube Windows 365 adecuado para usted.

Administración de oportunidades con Sales Advisor

¿Cuál es la funcionalidad de Sales Advisor en Microsoft 365 Lighthouse y cuál es la propuesta de valor empresarial para los asociados?

Comprender cómo los clientes interactúan con un producto o una solución a través de datos puede ayudar a los asociados a anticipar las necesidades de los clientes y mejorar el rendimiento general en las distintas fases del ciclo de vida del cliente. Microsoft está invirtiendo en sus asociados mediante la creación de una herramienta que admita una experiencia de administración del ciclo de vida de los clientes (CLM) y la participación continua del cliente en todo el ciclo de vida del cliente. Esta experiencia estaba disponible durante una fase de versión preliminar pública y se denominaba "Project Orland for Microsoft 365". La fase de versión preliminar pública ha finalizado y esta misma experiencia ahora está disponible con carácter general como una funcionalidad dentro de Microsoft 365 Lighthouse.

Aprovechando los mismos modelos de datos e información que los vendedores de Microsoft usan para la administración de cuentas, los partners pueden:

1. Dirija la participación del cliente en el momento adecuado con las acciones adecuadas.
2. Engage con los clientes cuando estén listos para el siguiente paso de su transformación digital en función de sus patrones de uso.
3. Obtenga una advertencia temprana de los clientes en los que la interacción directa puede evitar la renovación futura de Microsoft 365.
4. Acceda a contenido de marketing personalizado (como lanzamientos), información de uso y más específico para cada oportunidad de cliente expuesta dentro de la experiencia.
5. Aproveche las recomendaciones de procedimientos recomendados de Microsoft.

¿Qué segmentos de cliente ofrece la funcionalidad de Sales Advisor en Microsoft 365

Lighthouse soporte técnico? ¿Solo se debe usar con SME?

Sales Advisor presenta oportunidades en todos los segmentos. Las oportunidades y los modelos no son exclusivos de los clientes SMB. Los asociados de CSP que admiten clientes de tamaño medio encontrarán que Sales Advisor les sirve bien con todos los clientes con los que se involucran.

¿La funcionalidad de Sales Advisor en Microsoft 365 Lighthouse solo para Microsoft 365 o también está disponible para Azure y BizApps?

La funcionalidad Microsoft 365 Lighthouse Sales Advisor solo admite soluciones y servicios de Microsoft 365 de trabajo moderno.

Una vez que un asociado se incorpora a Lighthouse, ¿cómo comienza a trabajar con Sales Advisor?

Las instrucciones sobre cómo incorporarse a Lighthouse y cómo usar las funcionalidades de Sales Advisor se publican en Obtener acceso a Sales Advisor.

¿Cuál es la diferencia entre Sales Advisor y Cloud Ascent? ¿Son gratuitos?

Las dos ofertas sirven para diferentes propósitos y usan señales diferentes para generar información compartida con los asociados.

Cloud Ascent es una herramienta de orientación que se centra en los clientes potenciales de la nube que los asociados pueden trasladar a la nube. Los partners deben usar Cloud Ascent para admitir la generación de clientes potenciales y el nuevo marketing de clientes.

Para los clientes con una suscripción de prueba o de pago de Microsoft 365, la funcionalidad de asesor de ventas en Microsoft 365 Lighthouse ayudará a los asociados a nutrir a ese cliente mediante la conversión de las pruebas en de pago, el aumento de la adopción de productos o el traslado de clientes de pago a cargas de trabajo más avanzadas. Es una herramienta de administración del ciclo de vida que admite la participación continua del cliente. El asesor de ventas aprovecha los mismos modelos de

datos, información y señales que los vendedores de Microsoft usan para la administración de cuentas, aprovechando los procedimientos recomendados que se ven en todo el mercado para ayudar a los partners a hacer crecer su negocio.

Otras soluciones de administración multiinquilino

¿Cuál es la diferencia entre Microsoft 365 Lighthouse y Azure Lighthouse?

Microsoft 365 Lighthouse se centra en los servicios de Microsoft 365 en lugar de en los servicios de Azure. Aunque Azure Lighthouse está integrado en la Azure Portal y permite a los asociados de TI administrar varios inquilinos para Azure, Microsoft 365 Lighthouse es un portal independiente que ayuda a los MSP a administrar varios inquilinos de clientes de Microsoft 365. Para obtener más información sobre Microsoft 365 Lighthouse, consulte Información general de Microsoft 365 Lighthouse. Para obtener más información sobre Azure Lighthouse, consulte ¿Qué es Azure Lighthouse?

¿Cómo afecta Microsoft 365 Lighthouse a la actividad notificada por Microsoft Sentinel?

Microsoft 365 Lighthouse orígenes y agrega información de los inquilinos de los clientes a través de las API de Microsoft Graph. Si Microsoft Sentinel supervisa los inquilinos de clientes administrados por Lighthouse, detectará dicha actividad de API y, en función de cómo se configure Microsoft Sentinel, la notificará como un incidente. Puede crear una regla de automatización en Microsoft Sentinel para identificar estos incidentes como falsos positivos y cerrarlos automáticamente. Para obtener instrucciones sobre cómo hacerlo, consulte Control de falsos positivos en Microsoft Sentinel. Para más información sobre Microsoft Sentinel, revise la documentación técnica de Microsoft Sentinel.

¿Cuál es la diferencia entre Microsoft 365 Lighthouse y las capacidades de organización multiinquilino en Microsoft Defender XDR? Si administro servicios para LASB, ¿qué debo usar?

Las funcionalidades multiinquilino de Microsoft Defender XDR proporcionan a las organizaciones grandes la capacidad de proteger y administrar varios inquilinos desde

un único portal, con un enfoque en los flujos de investigación del Centro de operaciones de seguridad global (SOC), incluida una vista unificada de incidentes entre inquilinos y la capacidad de realizar búsquedas avanzadas en los datos contenidos en varios inquilinos. Las funcionalidades también ayudan a los proveedores de servicios de seguridad administrados (MSSP) empresariales a ejecutar de forma eficaz su SOC.

Para los MSP que administran servicios para clientes SMB y que necesitan un conjunto completo de funcionalidades que abarcan la seguridad, la identidad y la administración de aplicaciones de Microsoft 365 en una experiencia unificada en un único portal, seguimos recomendando Microsoft 365 Lighthouse. Lighthouse incluye un conjunto más amplio de funcionalidades optimizadas para los CSP, especialmente las que usan Microsoft 365 Empresa Premium y Defender para Empresas.

En la tabla siguiente se proporciona una comparación entre Microsoft 365 Lighthouse y las funcionalidades de la organización multiinquilino en Microsoft Defender XDR.

Expandir tabla

	Microsoft 365 Lighthouse	**Funcionalidades de organización multiinquilino en Microsoft Defender XDR**
Enfoque de audiencia y solución	Los CSP inscritos en el programa CSP, especialmente los que se centran en soluciones SMB como Defender para Empresas y Microsoft 365 Empresa Premium Incluye un conjunto completo de funcionalidades que abarcan la seguridad, la identidad y la administración de aplicaciones de Microsoft 365 en una experiencia unificada en un único portal	Grandes organizaciones de clientes y MSSP centrados en clientes empresariales Ayuda a los CSP a administrar de forma eficaz sus operaciones de seguridad Microsoft Defender XDR proporcionando la capacidad de ver incidentes y alertas, buscar amenazas y abordar escenarios de seguridad avanzada desde un único portal
Requisitos de idoneidad	Los CSP deben inscribirse en el programa CSP.	Requiere una relación GDAP con el cliente

	Microsoft 365 Lighthouse	Funcionalidades de organización multiinquilino en Microsoft Defender XDR
	Requiere una relación de acceso delegado con el cliente Consulte la lista completa de requisitos.	Clientes que usan Microsoft Entra colaboración B2B
Gorra de asiento	Hasta 2500 puestos por inquilino administrado	Ilimitado
Límite de inquilino	Ilimitado	Hasta 50 inquilinos por cliente o asociado
Aprovisionamiento de inquilinos en Defender para Empresas o Defender para punto de conexión	Iniciado mediante el aprovisionamiento con un solo clic en la línea base predeterminada en Lighthouse	Iniciado seleccionando **Dispositivos activos**> en el portal de Microsoft Defender del cliente
Incorporación a Defender para Empresas o Defender para punto de conexión	Se realiza a través de la línea base predeterminada en Lighthouse para dispositivos inscritos en Intune	Los dispositivos se pueden incorporar en el portal de Microsoft Defender de cada cliente o mediante Intune
Capacidad de ver el estado de licencia	Visible a través de la línea base predeterminada en Lighthouse	Visible en el portal de Microsoft Defender de cada cliente
Inventario de dispositivos	Ver todos los dispositivos (todas las plataformas) inscritos en Intune o dispositivos Windows incorporados a Defender para Empresas o Defender para punto de conexión	Ver una lista de inquilinos e información sobre dispositivos (Windows, iOS, Android, Mac, Linux) incorporados a Defender para Empresas o Defender para punto de conexión
Administración de configuración entre puntos de conexión,	Implemente las configuraciones recomendadas en los	Planeada para una versión futura

	Microsoft 365 Lighthouse	Funcionalidades de organización multiinquilino en Microsoft Defender XDR
correo electrónico, Intune, identidad, protección de datos	inquilinos a través de la línea base predeterminada, incluidas las directivas de reducción de superficie expuesta a ataques, firewall y antivirus, así como correo electrónico, Intune, etc. Detectar configuraciones que ya están presentes en el inquilino y variaciones de la configuración recomendada Informes multiinquilino sobre implementaciones entre inquilinos	
Administración de amenazas y vulnerabilidades	Vista agregada de la puntuación de exposición, la mayoría de los dispositivos expuestos y las recomendaciones entre inquilinos	Vista agregada de la puntuación de exposición y la mayoría de los dispositivos expuestos
Incidentes y alertas	Visualización de incidentes y alertas, con vínculos a inquilinos individuales para ver detalles y realizar acciones Acciones masivas para asignar o resolver un incidente o una alerta Notificaciones automatizadas por correo electrónico de incidentes y alertas basadas en reglas personalizables	Visualización de incidentes y alertas, con vínculos a inquilinos individuales para ver detalles y realizar acciones Acciones masivas para asignar o resolver un incidente o una alerta

	Microsoft 365 Lighthouse	Funcionalidades de organización multiinquilino en Microsoft Defender XDR
Búsqueda avanzada de amenazas	No disponible	Búsqueda de amenazas en varios inquilinos simultáneamente **Nota:** La búsqueda avanzada solo está disponible en Microsoft Defender para punto de conexión P2
Búsqueda global	Búsqueda global de usuarios y dispositivos administrados entre inquilinos	Búsqueda global de archivos, usuarios y dispositivos entre inquilinos
Puntuación de seguridad de Microsoft	Vista comparativa de puntuación segura en todos los inquilinos administrados	No disponible
Identity	Usuarios marcados por Protección de Microsoft Entra ID de comportamiento de riesgo entre inquilinos, incluida la capacidad de corregir riesgos de forma masiva Cuentas de usuario inactivas y cuentas de buzón compartido desprotegidas, incluida la capacidad de bloquearlas Habilitación de la autenticación multifactor y finalización del registro entre inquilinos Habilitación del autoservicio de restablecimiento de	No disponible

	Microsoft 365 Lighthouse	Funcionalidades de organización multiinquilino en Microsoft Defender XDR
	contraseña y finalización del registro entre inquilinos	
Administración	Lista de todos los dispositivos inscritos en Intune y su estado de cumplimiento de dispositivos Información de estado de dispositivos y aplicaciones para dispositivos inscritos en Intune de Análisis de puntos de conexión Lista de dispositivos PC en la nube Windows 365 y acciones básicas de administración	No disponible
Otras funcionalidades de seguridad	Lista de dispositivos inscritos en Intune que están vencidos por exámenes o que no tienen Microsoft Defender Antivirus o las últimas actualizaciones Microsoft Defender Antivirus Información sobre los correos electrónicos en cuarentena entre inquilinos Vista agregada de incidentes y avisos de mantenimiento del servicio entre inquilinos	No disponible
Asesor de ventas	Conclusiones, recomendaciones e instrucciones basadas en IA para ayudar a los CSP a	No disponible

	Microsoft 365 Lighthouse	Funcionalidades de organización multiinquilino en Microsoft Defender XDR
	adquirir, conservar y aumentar los clientes	

Obtener ayuda y proporcionar comentarios

Cómo obtener ayuda y soporte técnico?

En Lighthouse, seleccione el icono **?** en la parte superior del portal o el widget **De ayuda & soporte técnico** en la esquina inferior derecha del portal para abrir el panel **Ayuda** . Desde aquí, seleccione **Ayuda y soporte técnico** para acceder a artículos de autoayuda o póngase en contacto con el soporte técnico. Para obtener más información sobre las opciones de ayuda y soporte técnico, consulte Obtener ayuda y soporte técnico para Microsoft 365 Lighthouse.

¿Dónde puedo enviar comentarios e ideas?

¡Sus comentarios son importantes y son importantes para nosotros! Hay varias maneras diferentes de enviar comentarios:

- En Lighthouse, seleccione el widget **Dar comentarios** en la esquina inferior derecha del portal.
- Vaya a la página comentarios de Microsoft 365 Lighthouse. Puede iniciar conversaciones sobre Lighthouse y Windows 365 características, publicar preguntas para otros MSP o empleados de Microsoft, proporcionar comentarios e ideas de características, etc.
- Responda a la ventana emergente ocasional (no más de una vez al mes) en Lighthouse que le pide que proporcione comentarios.

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Privacidad y cumplimiento de datos en Microsoft 365 Lighthouse

Artículo • 11/10/2024

La privacidad de los datos es la protección de los datos frente al uso indebido. También es la capacidad de una persona para decidir cómo se recopilan, comparten, almacenan y usan los datos personales. En el mundo actual, la privacidad de los datos es una preocupación crítica porque puede afectar a la reputación, la seguridad y la confianza de todos los implicados. Al garantizar el derecho de una persona a controlar sus datos personales, las organizaciones no solo pueden proteger la información confidencial, sino también mantener una reputación positiva y cumplir las expectativas de transparencia y confianza.

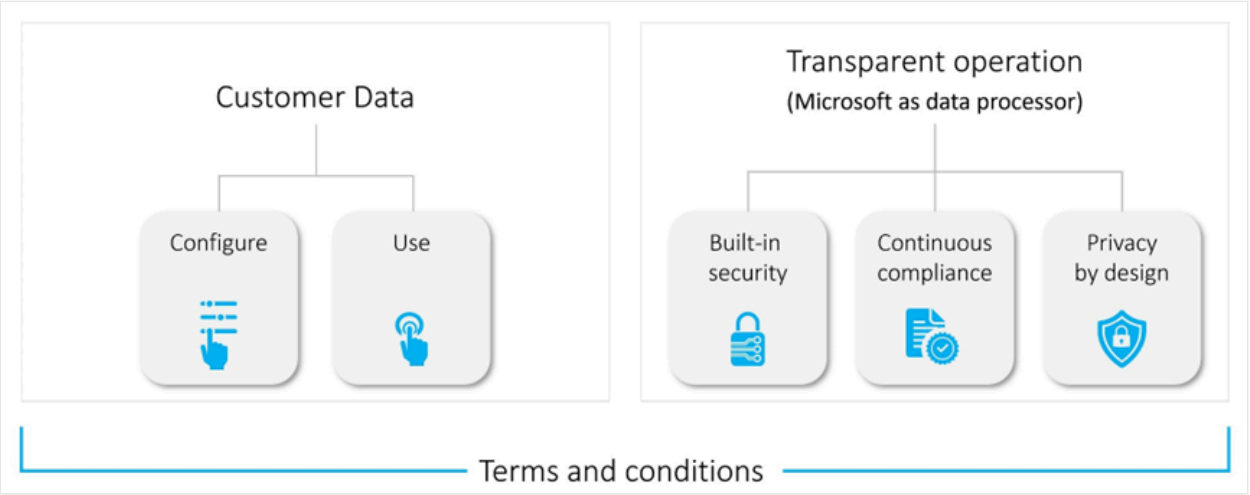
> ⓘ **Nota**
>
> Este artículo no sustituye el asesoramiento jurídico profesional. Debe consultar a su asesor legal para obtener instrucciones específicas sobre el cumplimiento de las regulaciones de privacidad.

Responsabilidad compartida

Microsoft y los proveedores de servicios administrados (MSP) comparten la responsabilidad de la protección de datos al usar datos en Lighthouse. Ambas partes deben garantizar que la protección de datos se alinee con los términos y condiciones de Microsoft y cumpla con las normativas pertinentes. Los roles y responsabilidades de protección de datos son los siguientes:

- Microsoft es responsable de proporcionar el servicio Lighthouse y asegurarse de que es compatible y seguro.
- Los MSP son responsables de usar los datos del cliente de forma responsable y transparente.
- Los clientes son responsables de conceder y revocar las relaciones que proporcionan a su MSP acceso a los datos.

Este enfoque de colaboración garantiza que todas las partes implicadas tomen las medidas necesarias para proteger los datos y mantener los estándares más altos de privacidad de los datos.



Acceso a los datos

El acceso a datos es la capacidad autorizada para acceder a los datos y usarlos. A la hora de acceder a datos en Lighthouse, Microsoft sigue varios principios clave:

- **Apertura:** Microsoft cree en la apertura y la colaboración. Los datos deben ser accesibles para todos los usuarios que los necesiten, y deben fomentar la innovación e informar a la toma de decisiones. Las iniciativas de datos abiertos promueven la transparencia y permiten la colaboración entre organizaciones.
- **Usabilidad:** El acceso a los datos debe ser sencillo y fácil de usar. Microsoft proporciona herramientas, API e interfaces que permiten a los desarrolladores y usuarios interactuar con los datos de forma eficaz. La facilidad de uso garantiza que los datos sean accesibles sin complejidad innecesaria.
- **Empoderamiento:** El acceso a datos permite a las personas, organizaciones y comunidades. La habilitación del acceso a los datos pertinentes permite a Microsoft contribuir a resolver los desafíos del mundo real y tener un impacto positivo en la sociedad.
- **Seguridad:** Microsoft prioriza la seguridad al promover el acceso a datos. Los sólidos mecanismos de autenticación, autorización y cifrado protegen los datos del acceso no autorizado. Las medidas de seguridad garantizan que los datos sigan siendo confidenciales e integrales.
- **Privacidad:** Respetar la privacidad del usuario es fundamental. Microsoft se adhiere a las regulaciones de privacidad y a los procedimientos recomendados. El acceso a los datos no debe poner en peligro los derechos de privacidad individuales y los datos personales deben controlarse de forma responsable.

Estos principios guían el enfoque de Microsoft para el acceso a datos. Hacen hincapié en el uso compartido y la colaboración responsables y fomentan la innovación, a la vez que protegen la privacidad y la seguridad.

Relaciones de acceso a datos

En Lighthouse, las relaciones de acceso a datos desempeñan un papel fundamental en la forma en que los CSP interactúan con los datos de los clientes. Estas relaciones definen la base para el control de datos éticos y transparentes. Los dos tipos clave de relación de acceso a datos de Lighthouse incluyen:

- **Relación de administrador delegado**
  - **Rol:** Los administradores delegados realizan tareas administrativas en nombre de los clientes para respaldar el éxito de los clientes.
  - **Propósito:** Este tipo de relación simplifica las acciones rutinarias, como la administración de usuarios y la supervisión del servicio.
  - **Valor añadido:** Los permisos específicos garantizan un acceso controlado.

- **Relación de revendedor**
  - **Rol:** Los revendedores actúan como intermediarios entre los servicios de Microsoft y los usuarios.
  - **Propósito:** Administran licencias, facturación y otros servicios.
  - **Valor añadido:** A menudo, los revendedores proporcionan soporte y experiencia adicionales.

La relación de revendedor se establece para autorizar a los MSP a administrar pedidos y compras para el cliente. Esta disposición proporciona a los MSP visibilidad sobre las suscripciones que el cliente ha adquirido a través de ellas, lo que garantiza que pueda admitir y atender esas suscripciones de forma eficaz. Los cambios en la relación de revendedor pueden tardar 24 horas o más en reflejarse en Lighthouse. Este período de tiempo de procedimiento no afecta al conocimiento preexistente de las suscripciones de un MSP.

A diferencia de la relación de revendedor, la relación de administrador delegado se establece para autorizar a los MSP a acceder y administrar los datos y recursos del cliente. Esta relación se basa en el consentimiento del cliente y se puede revocar en cualquier momento. Los cambios en la relación de administración delegada se reflejan inmediatamente en Lighthouse, lo que garantiza que el acceso a los datos del cliente está protegido de acuerdo con los privilegios que el cliente ha concedido al MSP. Esto es especialmente importante para escenarios como la respuesta a incidentes de seguridad, donde el acceso a datos puntual y preciso es fundamental.

Estas relaciones garantizan que los CSP accedan a los datos de forma responsable, a la vez que mejoran la satisfacción del cliente. Al comprender y optimizar estas conexiones, las organizaciones pueden crear un ecosistema de datos sólido.

Áreas de características de datos

Las relaciones de acceso a datos se intersecan con las siguientes áreas de características de datos:

- **Conclusiones de éxito del cliente**
  Estas características incluyen oportunidades y renovaciones de suscripciones y permiten a los CSP ofrecer orientación proactiva y recomendaciones a sus clientes.
  - **Origen de datos:** Lighthouse usa datos de uso anonimizados de nivel de inquilino, que combinan información de suscripción con información agregada. Este enfoque garantiza análisis valiosos al tiempo que protege la privacidad individual. Lighthouse expone la información de éxito del cliente de los clientes que tienen una relación de revendedor activa o una relación de administrador delegado con el MSP.
  - **Ejemplo:** Mediante el uso de la característica de renovación de suscripciones, un MSP puede conectarse proactivamente con su cliente para analizar sus necesidades y tomar las medidas adecuadas para evitar una interrupción del servicio.

- **Administración de clientes**
  Estas características ayudan a los MSP a supervisar y administrar los datos de los clientes, los dispositivos y los usuarios.
  - **Origen de datos:** Lighthouse recopila datos de clientes que tienen una relación de administrador delegado activo con el MSP y cuyo inquilino se incorporó correctamente a Lighthouse.
  - **Ejemplo:** Mediante el uso de la característica de cumplimiento de dispositivos, un MSP puede evaluar el estado de los dispositivos del cliente e identificar cualquier problema que afecte a la productividad y la seguridad.

Al comprender estas áreas de características y su conexión a las relaciones de acceso a datos, las organizaciones pueden navegar por los datos de forma responsable, a la vez que mejoran la satisfacción del cliente.

Residencia de datos

La residencia de datos hace referencia a la ubicación física donde se almacenan y procesan los datos. La privacidad de los datos, las leyes de protección y las regulaciones pueden variar según la región y el país, y algunos clientes pueden preferir o requerir que sus datos residan en determinadas ubicaciones. Los MSP deben comprender cómo Lighthouse controla la residencia de datos y qué opciones están disponibles para ellos y sus clientes.

Lighthouse procesa y almacena datos de acuerdo con las leyes y regulaciones regionales de protección de datos. Sin embargo, es importante tener en cuenta que Lighthouse tiene diferentes compromisos de residencia de datos que otros servicios de Microsoft 365. Por ejemplo, algunos servicios de Microsoft 365 permiten a los clientes elegir un país específico para su procesamiento y almacenamiento de datos, mientras que Lighthouse no ofrece esta opción. Los MSP y los clientes deben tener en cuenta que Lighthouse procesa y almacena datos en la región asociada al inquilino del cliente.

Este enfoque está diseñado para proporcionar una experiencia coherente y unificada para los CSP que administran clientes en diferentes regiones. Al procesar y almacenar datos en la región del inquilino del cliente, Lighthouse puede optimizar el rendimiento, la confiabilidad y la escalabilidad de estos MSP.

Para obtener más información sobre cómo Lighthouse controla la recopilación de datos, consulte Recopilación de datos para Microsoft 365 Lighthouse.

Eliminación de datos

Los datos disponibles en Lighthouse desempeñan un papel importante en las características y funciones valiosas que Lighthouse proporciona para los MSP, como experiencias optimizadas de administración de inquilinos e información sobre el éxito de los clientes. ¿Pero qué ocurre si desea quitar los datos de Lighthouse? ¿Cómo se quita y cuáles son las consecuencias?

La eliminación de datos es el proceso de retirar el permiso para acceder a los datos y usarlos que se concedieron anteriormente a un servicio. La eliminación de datos también puede implicar detener el acceso y el uso de los datos que ya almacena el servicio. Esto se puede hacer sin afectar a la relación de un MSP con su cliente, ya que el MSP todavía puede realizar otras acciones administrativas en nombre del cliente. La eliminación de datos es un aspecto crucial de la gobernanza de los datos, ya que permite a los csp y clientes controlar sus datos y proteger su privacidad y seguridad.

Eliminación de datos para inquilinos asociados

Los MSP controlan si Lighthouse puede acceder a sus datos y usarlos. Para quitar sus datos de Lighthouse, los MSP pueden realizar una de las siguientes acciones:

- Póngase en contacto con Soporte técnico de Microsoft, que procesará el inquilino del asociado para su retirada del servicio Lighthouse.
- Quite las entidades de servicio para Microsoft 365 Lighthouse por sí mismas, si tienen experiencia en la administración de entidades de servicio y Microsoft Entra ID.

Al realizar una de estas acciones, los MSP pueden mantener el control sobre sus datos y, al mismo tiempo, interrumpir el uso de Lighthouse. Estas acciones dan como resultado la pérdida de acceso a las características y funciones proporcionadas por Lighthouse, como las experiencias de administración de inquilinos y la información de éxito del cliente.

Eliminación de datos para inquilinos de clientes

Los clientes controlan si Lighthouse puede acceder a sus datos y usarlos. La retirada de la capacidad de Lighthouse para acceder a los datos del cliente y usarlos puede afectar a la capacidad del MSP de administrar y proteger de forma eficaz el inquilino del cliente. Antes de realizar cambios en el acceso a los datos, los clientes deben tener en cuenta lo siguiente:

- Lighthouse podría ser la solución que su MSP eligió para proporcionar los servicios administrados que el cliente compró del MSP.
- Lighthouse ya no podrá proporcionar al MSP información valiosa sobre la configuración del inquilino del cliente y podrían surgir posibles problemas de seguridad como resultado.

Si un MSP quiere impedir que Lighthouse acceda a los datos del cliente y los use, este puede desactivar el inquilino del cliente. La inactivación puede ser un enfoque útil, ya que no afecta a la relación de administrador delegado o de revendedor entre el cliente y el MSP. Para desactivar un inquilino de cliente, los CSP deben seguir estos pasos:

1. En el panel de navegación izquierdo de Lighthouse, seleccione **Inquilinos** para abrir la página **Inquilinos** .
2. Busque el inquilino que desea desactivar, seleccione los tres puntos (más acciones) junto al nombre del inquilino y, a continuación, seleccione **Inactivar inquilino**.
3. En el cuadro de diálogo de confirmación, seleccione **Confirmar** para desactivar el inquilino.

Como alternativa, el cliente puede retirar la capacidad del MSP de acceder a los datos del cliente o usarlos finalizando la relación de administrador delegado y la relación de revendedor que tiene con el MSP. Antes de quitar cualquiera de las relaciones, es importante tener en cuenta lo siguiente:

- La eliminación de la relación de administrador delegado significa que el MSP ya no puede realizar acciones de administración en nombre del cliente, como configurar servicios, restablecer contraseñas y mucho más.
- La eliminación de la relación de revendedor significa que el MSP cancelará las suscripciones que el cliente compró a través del MSP.

Restricciones de datos

La privacidad y el cumplimiento de los datos son aspectos importantes del uso de datos en Lighthouse. Las restricciones de datos se basan en los términos y condiciones del producto y en los contratos que se aplican al programa Proveedor de soluciones en la nube. Estos acuerdos pueden cambiar de vez en cuando, y es responsabilidad del MSP seguirlos y consultar con el asesor legal según sea necesario.

Las restricciones de datos limitan el uso de datos. Por ejemplo, los datos no se pueden usar con fines de marketing o ventas. Los CSP pueden usar datos en Lighthouse solo con fines de éxito del cliente y solo si no infringen las restricciones de datos o las preferencias de privacidad del cliente. *Los propósitos de éxito del cliente* garantizan que los clientes logran sus resultados deseados mientras usan un producto o servicio. *Los fines de marketing y ventas* implican persuadir a los clientes de comprar un producto o servicio.

Algunos ejemplos de cómo se pueden usar los datos para el éxito del cliente incluyen:

- Proporcionar comunicaciones y comentarios pertinentes y oportunos a los clientes.
- Ayudar a los clientes a adoptar y usar las características y funcionalidades que mejor se adapten a sus necesidades y objetivos.
- Proporcionar a los clientes valor adicional o servicios que mejoren su experiencia y resultados con Microsoft servicios en línea.
- Proporcionar orientación proactiva y soporte técnico a los clientes para resolver problemas y evitar problemas.

Retención de datos

Lighthouse sigue diferentes directivas de retención de datos para los distintos tipos de datos que recopila de los inquilinos de asociados y clientes. En la tabla siguiente se resumen las directivas de retención de datos para cada tipo de datos, el método de eliminación y los principios seguidos.

Expandir tabla

Tipo de datos	Período de retención	Método de eliminación	Principios seguidos
Datos recopilados de inquilinos de clientes	30 días	Automático	Minimización de datos, transparencia y responsabilidad

Tipo de datos	Período de retención	Método de eliminación	Principios seguidos
Datos generados por los MSP mediante el uso del servicio Lighthouse	Hasta que el MSP lo elimine o hasta que el cliente o EL MSP se desborde	Manual	Control de usuario, consentimiento
Datos de diagnóstico recopilados de los CSP	30 días	Automático	Minimización de datos, transparencia y responsabilidad

Las directivas de retención de datos están diseñadas para minimizar la cantidad de datos de clientes que se almacenan fuera de los inquilinos del cliente, a la vez que proporcionan información valiosa y acciones para los CSP. Las directivas también están diseñadas para ayudar a los MSP a administrar a sus clientes de forma eficaz y eficaz. Las directivas de retención de datos siguen los principios de minimización de datos, transparencia, responsabilidad, control de usuario, consentimiento y elección al administrar datos.

Los MSP y los clientes no pueden configurar períodos de retención de datos. Cuando Lighthouse elimina datos que tienen más de 30 días, se borran permanentemente del servicio y no se pueden recuperar. Los datos no se almacenan ni transfieren a ninguna otra ubicación o servicio.

Para obtener más información, consulte Retención, eliminación y destrucción de datos en Microsoft 365.

Contenido relacionado

Centro de confianza de Microsoft (página de vínculos)
Privacidad en Microsoft (página de vínculo)
Recopilación de datos para Microsoft 365 Lighthouse (artículo)
Retención, eliminación y destrucción de datos en Microsoft 365 (artículo)
Centro de cumplimiento de Microsoft (página de vínculo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto

Recopilación de datos para Microsoft 365 Lighthouse

Artículo • 11/10/2024

La recopilación de datos es la forma en que Microsoft 365 Lighthouse recopila y analiza información de proveedores de servicios administrados (MSP) y clientes. El servicio Lighthouse recopila datos a través del uso de MSP y las operaciones de servicio a servicio para los clientes con los que un MSP tiene una relación de administrador delegado. Con estos datos, Lighthouse puede proporcionar al MSP información valiosa y recomendaciones adaptadas, y habilitar la administración centralizada desde una sola experiencia.

Recopilación de datos para MSP

Lighthouse recopila datos de los MSP cuando un usuario del inquilino asociado usa Lighthouse. Estos datos ayudan a Lighthouse a proporcionar y mejorar su servicio para los clientes y MSP específicos implicados. Estos datos no se comparten con otras partes y están protegidos por estrictas medidas de privacidad y seguridad. El MSP tiene control y propiedad completos sobre sus datos, y pueden verlos, administrarlos o eliminarlos en cualquier momento. Los datos recopilados de los inquilinos de asociados se dividen en dos categorías: datos de diagnóstico y datos de uso.

- **Datos de diagnóstico:** Estos datos capturan el rendimiento y la confiabilidad de Lighthouse, como errores, bloqueos o errores. Los datos de diagnóstico ayudan a identificar y resolver problemas que afectan a la calidad del servicio o a la experiencia del usuario.
- **Datos de uso:** Estos datos reflejan las acciones y preferencias del asociado al usar Lighthouse, como especificar contactos o sitios web para los clientes, crear líneas base personalizadas, implementar tareas de implementación o configurar relaciones de privilegios administrativos delegados granulares (GDAP). Los datos de uso ayudan a Lighthouse a personalizar y optimizar el servicio para cada MSP en función de su entrada.

Algunos ejemplos de los datos de diagnóstico que se recopilan son:

- **Errores:** Estos datos capturan errores como errores de servicio que se producen cuando un MSP usa Lighthouse. Los datos de error ayudan a Lighthouse a diagnosticar y corregir los problemas que impiden que el MSP use el servicio correctamente.

- **Fallas:** Estos datos capturan los errores que se producen cuando un asociado usa Lighthouse, como errores de línea base o errores de implementación. Los datos de error ayudan a Lighthouse a comprender y mejorar la tasa de éxito y la calidad de las funciones y características del servicio.
- **Métricas de rendimiento:** Estos datos capturan el rendimiento de Lighthouse, como el tiempo de carga, el tiempo de respuesta o el rendimiento. Las métricas de rendimiento ayudan a Lighthouse a medir y optimizar la velocidad y eficiencia del servicio.

Algunos ejemplos de los datos de uso que Lighthouse recopila cuando un usuario autorizado de un inquilino asociado usa la experiencia son:

- **Creación de líneas base personalizadas:** Cuando un asociado crea una línea base personalizada en Lighthouse, Lighthouse almacena la información y la usa para asociar la línea base a uno o varios inquilinos de clientes.
- **Implementación de tareas de implementación:** Cuando un asociado implementa una tarea de implementación que forma parte de una línea base en Lighthouse, Lighthouse almacena esta información y la usa para realizar un seguimiento del progreso y el estado de la tarea de implementación. Esta información también se usa para notificar los errores o errores que se producen durante el proceso de implementación.
- **Especificar contactos o sitios web para clientes:** Cuando un asociado especifica un contacto o un sitio web para un cliente en Lighthouse, Lighthouse almacena esta información y la usa para mostrar los detalles del cliente en el panel.
- **Configuración de relaciones GDAP:** Cuando un asociado configura una relación GDAP con un inquilino de cliente en Lighthouse, Lighthouse almacena la información y la usa para configurar y administrar la relación GDAP. Esta información también se usa para comprobar el consentimiento y la autorización del cliente al acceder a sus datos. Esta información no se comparte con otras partes y está protegida por estrictas medidas de privacidad y seguridad.

Recopilación de datos para clientes de MSP

Lighthouse recopila datos de los inquilinos del cliente a través de un plan de servicio que le permite acceder a los datos del cliente con su consentimiento. El MSP también debe tener acceso delegado a la relación de administrador del delegado de inquilino del cliente.

Los datos recopilados de los inquilinos del cliente ayudan a Lighthouse a proporcionar una mejor seguridad y rendimiento para esos inquilinos. Por ejemplo, mediante la recopilación de información del dispositivo, Lighthouse puede ayudar al MSP a

identificar y resolver problemas que afectan a los dispositivos del cliente, como infecciones de malware, errores de hardware o actualizaciones de software. Microsoft respeta la privacidad y la seguridad de los datos recopilados de los inquilinos del cliente. Lighthouse usa directivas de cifrado, control de acceso, auditoría y retención para proteger los datos frente a usos o divulgaciones no autorizados o inadecuados.

En la tabla siguiente se resumen los tipos de datos que Lighthouse recopila de los inquilinos del cliente, de dónde los recopila, de qué ámbito trata y de qué propósito sirve.

Expandir tabla

Categoría de datos	Origen de datos	Ámbito de datos	Propósito de datos
Administración de equipos en la nube	Windows 365	Varios tipos de datos relacionados con la administración de usuarios y dispositivos de PC en la nube, como: • Metadatos de dispositivos de PC en la nube, como el nombre del dispositivo, el identificador de dispositivo, el grupo de dispositivos, el estado del dispositivo y la configuración del dispositivo • Metadatos de los usuarios del equipo en la nube, como el nombre de usuario, el identificador de usuario, el grupo de usuarios, el rol de usuario y la asignación de usuarios • Metadatos de conexiones de PC en la nube, como el nombre de conexión, el tipo de conexión, el estado de la conexión y los detalles de la conexión	Ayuda a los MSP a administrar dispositivos y usuarios de PC en la nube en los inquilinos de los clientes. Ayuda a los MSP a medir y mejorar el rendimiento del equipo en la nube y la experiencia del usuario en los inquilinos de los clientes.
Microsoft Copilot	Copilot Microsoft Entra	Varios tipos de datos relacionados con Copilot, como: • Uso de servicios de Copilot • Metadatos de suscripciones y recuento de asignaciones de licencias	Ayuda a los MSP a administrar la habilitación y adopción de Copilot entre los inquilinos del cliente. Ayuda a los MSP a

Categoría de datos	Origen de datos	Ámbito de datos	Propósito de datos
			mejorar la productividad y el éxito de los clientes mediante la inteligencia artificial.
Administración de dispositivos	Microsoft Intune	Varios tipos de datos relacionados con la inscripción de dispositivos, el cumplimiento de dispositivos, la protección de aplicaciones y la configuración de dispositivos, como: • Metadatos de dispositivos inscritos • Metadatos de directivas de protección de aplicaciones • Metadatos de perfiles de configuración de dispositivos Comparación del estado de cumplimiento de dispositivos y las directivas de protección de aplicaciones con la configuración de línea base	Ayuda a los MSP a administrar dispositivos entre inquilinos de clientes. Ayuda a los MSP a medir y mejorar el cumplimiento de los dispositivos y la protección de aplicaciones entre los inquilinos del cliente.
Rendimiento del dispositivo	Análisis de puntos de conexión	Metadatos del rendimiento del dispositivo, como el nombre del dispositivo, el identificador de dispositivo, el grupo de dispositivos, la puntuación de rendimiento de inicio, la frecuencia de reinicio, la duración del inicio de sesión, la duración de la batería y la confiabilidad de la aplicación Metadatos de recomendaciones de dispositivo, como nombre, tipo, impacto, estado y detalles	Ayuda a los MSP a administrar el rendimiento de los dispositivos entre los inquilinos del cliente. Ayuda a los MSP a medir y mejorar la productividad de los dispositivos y la experiencia del usuario en los inquilinos de los clientes.
Administración de aplicaciones* (versión preliminar)	Centro de Administración de Aplicaciones de Microsoft 365	Metadatos relacionados con la administración de aplicaciones de Microsoft 365, como el canal de actualización, el número de compilación y versión, y las aplicaciones y complementos de	Ayuda a los MSP a administrar el estado de las aplicaciones de Microsoft 365 en los inquilinos de los

Categoría de datos	Origen de datos	Ámbito de datos	Propósito de datos
		Microsoft 365 instalados. Metadatos de dispositivos de Office, como el sistema operativo, el almacenamiento, la RAM, la arquitectura del sistema (por ejemplo, 64 bits), el último usuario que inició sesión, los dispositivos en una compilación no admitida, los dispositivos que no están en la compilación más reciente y los dispositivos que usan la actualización en la nube.	clientes. Ayuda a los MSP a medir y mejorar la productividad de los dispositivos de Office y la experiencia del usuario de aplicaciones de Microsoft 365 en los inquilinos de los clientes.
seguridad de Email	Microsoft Defender para Office 365	Metadatos de mensajes en cuarentena, como remitente, destinatario, asunto, fecha, motivo de cuarentena y estado de lanzamiento Metadatos de amenazas de correo electrónico, como el tipo de amenaza, la gravedad de la amenaza y la acción de amenaza	Ayuda a los MSP a administrar los mensajes en cuarentena entre los inquilinos del cliente. Ayuda a los MSP a medir y mejorar la seguridad del correo electrónico y la lucha contra la suplantación de identidad (phishing) en los inquilinos de los clientes.
Administración de identidad y acceso	Exchange Online	Metadatos de buzones compartidos, como la dirección de correo electrónico y el nombre	Ayuda a los MSP a administrar buzones compartidos entre inquilinos de clientes.
Administración de identidad y acceso	Microsoft Entra	Varios tipos de datos relacionados con la administración de identidades y acceso, la seguridad y el cumplimiento, y la administración de dispositivos y usuarios, como: • Información de identidad de usuario e inquilino • Información de licencia de usuario e inquilino	Ayuda a los MSP a administrar diversos aspectos de Microsoft Entra entre los inquilinos del cliente. Ayuda a los MSP a medir y mejorar la administración de

Categoría de datos	Origen de datos	Ámbito de datos	Propósito de datos
		• Información de seguridad de usuarios e inquilinos • Información de MFA/SSPR de usuario • Directivas de acceso condicional • Usuarios de riesgo • Información de usuario y grupo para la asignación Comparación de datos Microsoft Entra con la configuración de línea base	identidades y acceso, la seguridad y el cumplimiento, y la administración de dispositivos y usuarios en los inquilinos del cliente.
Posición de seguridad	Puntuación de seguridad de Microsoft	Todas las recomendaciones y acciones de seguridad	Ayuda a los MSP a evaluar y mejorar la posición de seguridad de los inquilinos del cliente.
Protección contra amenazas	Microsoft Defender para Empresas	Metadatos de dispositivos inscritos, como el nombre del dispositivo, el tipo de dispositivo y el identificador de dispositivo Metadatos de información sobre amenazas y vulnerabilidades, como nombre de amenaza (por ejemplo, Troyano: Win32/Emotet), gravedad de la amenaza (por ejemplo, alta), categoría de amenaza (por ejemplo, malware), estado de amenaza (por ejemplo, activo o resuelto), acción de amenaza (por ejemplo, cuarentena o permitir), nombre de vulnerabilidad (por ejemplo, CVE-2021-1234), gravedad de vulnerabilidad (por ejemplo, crítica), categoría de vulnerabilidad (por ejemplo, ejecución remota de código), puntuación de exposición de vulnerabilidad (por ejemplo, 8,5 de 10) y estado de corrección de vulnerabilidad (por ejemplo, pendiente o completada)	Ayuda a los MSP a supervisar y proteger los dispositivos frente a amenazas. Ayuda a los MSP a medir y mejorar la seguridad de los dispositivos y la administración de vulnerabilidades en los inquilinos de los clientes.

* Esta categoría de datos está en versión preliminar, no se aplica a todos y está sujeta a cambios.

No se recopilaron datos

Lighthouse permite a los MSP crecer, administrar y proteger a sus clientes de Microsoft 365 de forma más eficaz y eficiente. Para ello, Lighthouse recopila datos solo con fines específicos, como mejorar la confiabilidad, el mantenimiento y la escalabilidad del servicio de las aplicaciones y servicios de Microsoft 365. Microsoft también cumple con estándares estrictos para controlar los datos de forma segura y responsable.

Lighthouse nunca recopilará datos que no sean necesarios ni pertinentes para su servicio. Lighthouse no hará nada para poner en peligro la seguridad o la integridad de sus MSP y clientes. A continuación se muestran ejemplos de datos que Lighthouse nunca recopilará:

- **Datos biométricos:** Datos que identifican o comprueban la identidad de los CSP y clientes en función de sus características físicas o de comportamiento, como huellas digitales, reconocimiento facial, reconocimiento de voz o exámenes de iris.
- **Contenido de correos electrónicos, mensajes y documentos:** Datos que los MSP y los clientes crean, envían, reciben o almacenan en sus aplicaciones de correo electrónico, chat o documento.
- **Credenciales, contraseñas o claves:** Datos que los MSP y los clientes usan para acceder a sus cuentas, dispositivos o aplicaciones.
- **Datos de inquilinos de clientes inactivos:** Datos de administración de inquilinos de clientes que el MSP ha desactivado en Lighthouse.
- **Datos de relaciones de administración delegada inactivas:** Datos de inquilinos de clientes en los que el MSP no tiene una relación de administrador delegado activo.
- **Datos de ubicación:** Datos que revelan la ubicación física o geográfica de los MSP y los clientes, como coordenadas GPS, direcciones IP o redes Wi-Fi.
- **Información personal o financiera:** Datos que los partners y clientes pueden tener en sus perfiles, preferencias, transacciones o registros. Lighthouse garantiza que solo recopila los datos necesarios y pertinentes para su servicio y protege la privacidad y confidencialidad de sus proveedores de servicios y clientes.

Contenido relacionado

Centro de confianza de Microsoft (página de vínculos)
Privacidad en Microsoft (página de vínculo)

Comentarios

¿Le ha resultado útil esta página? Sí No

Proporcionar comentarios sobre el producto