Cyber Protect Cloud

23.02

Manual del administrador de socios

REVISIÓN: 28/02/2023

Contenido

Acerca de este documento **6**
Acerca de Cyber Protect **7**
Servicios de Cyber Protect 7
Modos de facturación para Cyber Protect 8
Conmutación entre ediciones y modos de facturación 10
Artículos de oferta y gestión de cuotas 13
Servicios y elementos de oferta 13
Uso del portal de gestión **26**
Navegadores web compatibles 26
Activación de la cuenta de administrador. 26
Requisitos de contraseña 26
Acceso al portal de gestión 27
Configuración de contactos en el asistente de Perfil de empresa 27
Acceso a la consola de Cyber Protection desde el portal de administración 28
Navegación en el portal de gestión 29
Limitación del acceso a la interfaz web 29
Acceso a los servicios 30
Pestaña General 30
Pestaña Clientes 31
Barra del historial de siete días 32
Las cuentas de usuario y los inquilinos 33
Gestión de inquilinos 35
Creación de un inquilino 35
Modo Seguridad aumentada 38
Pasos para gestionar los servicios para un inquilino 39
Configuración de los elementos de oferta para un inquilino 39
Habilitación de servicios para varios inquilinos existentes 40
Activación de las notificaciones de mantenimiento 42
Configuración del perfil del cliente administrado de forma automática 43
Configuración de los contactos de la empresa 43
Actualizar los datos de uso para un inquilino 46
Deshabilitación y habilitación de un inquilino 46
Mover un inquilino a otro inquilino 46
Conversión de un inquilino socio en un inquilino carpeta y viceversa 48
Limitación del acceso a su inquilino 48

Eliminación de un inquilino 49
Gestión de usuarios 50
Creación de una cuenta de usuario 50
Funciones de usuario disponibles para cada servicio 52
Cambiar los ajustes de notificaciones para un usuario 57
Deshabilitación y habilitación de una cuenta de usuario 59
Eliminación de una cuenta de usuario 60
Transferencia de la propiedad de una cuenta de usuario 60
Establecimiento de la autenticación de doble factor 61
Cómo funciona 61
Propagación de la configuración de doble factor en niveles de inquilino 62
Establecimiento de la autenticación de doble factor para el inquilino 64
Gestión de la autenticación de doble factor para usuarios 65
Restablecimiento de la autenticación de doble factor en caso de pérdida de dispositivo de segundo factor 67
Protección de fuerza bruta 67
Configuración de situaciones relacionadas con la venta de productos de gama superior a sus clientes 68
Puntos de venta de productos de gama superior que se muestran a un cliente 69
Gestión de ubicaciones y almacenamiento 70
Ubicaciones 70
Gestión de almacenamiento 71
Configuración del almacenamiento inmutable 72
Configuración de personalización de marca y etiquetado en blanco 75
Elementos de personalización de marca 76
Configuración de personalización de marca 78
Restaurar la configuración predeterminada de personalización de marca. 79
Deshabilitar la personalización de marca 79
Marcas blancas 79
Configuración de URL de la interfaz web personalizadas 80
Actualización de agentes automáticamente 81
Pasos para actualizar agentes automáticamente 81
Pasos para supervisar las actualizaciones de los agentes 83
Supervisión 83
Uso 83
Operaciones 83
Generación de informes 102

Uso ... 102
Informes de operaciones ... 105
Resumen ejecutivo ... 109
Zonas horarias de los informes ... 123
Datos informados según el tipo de widget ... 124
Registro de control ... 126
Campos del registro de control ... 127
Filtrado y búsqueda ... 128
Paquetes Advanced Protection ... 129
Características y paquetes avanzados incluidos en los servicios de Cyber Protect ... 130
Características avanzadas incluidas en el servicio de protección ... 130
Características avanzadas y de pago por uso en el servicio de protección ... 134
Prevención avanzada de la pérdida de datos ... 135
Habilitar la prevención avanzada de la pérdida de datos ... 135
Seguridad avanzada + EDR ... 136
Habilitar Seguridad avanzada + EDR ... 136
Recuperación ante desastres avanzada ... 137
Protección de correo electrónico avanzada ... 138
Integraciones ... 139
Integración con sistemas externos ... 139
Configuración de una integración de Cyber Protect Cloud ... 139
Gestión de clientes API ... 139
Referencias de integración ... 142
Integración con VMware Cloud Director ... 144
Limitaciones ... 145
Requerimientos de software ... 145
Configuración del agente de mensajes de RabbitMQ ... 146
Instalación del complemento para VMware Cloud Director ... 146
Instalación de un agente de gestión ... 147
Instalación de agentes de copia de seguridad ... 150
Actualización de agentes ... 152
Acceso a la consola web de Cyber Protection ... 153
Crear un administrador de copias de seguridad ... 154
Informe del sistema, archivos de registro y archivos de configuración ... 154
Eliminación de la integración con VMware Cloud Director ... 156
Configuración de privacidad ... 157
Índice ... 158

Acerca de este documento

Este documento está destinado a los administradores de partners que quieran utilizar Cyber Protect Cloud para proporcionar servicios a sus clientes.

En este documento se describe cómo configurar y gestionar los servicios disponibles en Cyber Protect Cloud mediante el portal de administración.

Acerca de Cyber Protect

Cyber Protect es una plataforma de la nube que permite a los proveedores de servicios, revendedores y distribuidores proporcionar servicios de protección de datos a sus partners y clientes.

Los servicios se proporcionan al nivel de socio, bajando hasta el nivel de la empresa cliente y el nivel de usuario final.

La gestión de servicios está disponible mediante las aplicaciones web denominadas **consolas de servicio**. La gestión de las cuentas de usuario e inquilino está disponible mediante una aplicación web denominada el **portal de administración**.

El portal de gestión permite a los administradores realizar las siguientes acciones:

- Monitorizar el uso de los servicios y acceder a las consolas de servicio
- Gestionar inquilinos
- Gestionar cuentas de usuario
- Configurar servicios y cuotas para inquilinos
- Gestionar almacenamiento
- Gestionar la personalización de marca
- Generar informes acerca del uso de los servicios

Servicios de Cyber Protect

Esta sección describe el conjunto de características presentado en marzo de 2021 con el nuevo modelo de facturación. Lea más acerca de las ventajas del nuevo modelo de facturación en la Ficha técnica de Cyber Protect.

Los siguientes servicios y conjuntos de características están disponibles en Cyber Protect Cloud:

- **Cyber Protect**
  - **Protección**: ciberprotección completa con funcionalidad de seguridad y gestión incluida en el producto base y recuperación ante desastres, copia de seguridad y recuperación, automatización y protección del correo electrónico disponibles como características de pago por uso. Esta funcionalidad puede ampliarse con los paquetes de protección avanzada sujetos a costes adicionales.
    Los paquetes de protección avanzada son conjuntos de características que engloban escenarios más sofisticados en un área funcional específica, por ejemplo, Advanced Backup, Advanced Security y otros. Los paquetes avanzados amplían la funcionalidad disponible en el servicio Cyber Protect estándar.
    Para obtener más información sobre los paquetes Advanced Protection, consulte "Paquetes Advanced Protection" (p. 129).

  - **File Sync & Share**: una solución para el uso compartido seguro de contenido corporativo desde cualquier parte, en cualquier momento y en cualquier dispositivo.
  - **Envío de datos físicos**: una solución que le ayuda a ahorrar tiempo y tráfico de red al enviar datos hacia el centro de datos de la nube mediante una unidad de disco duro.
  - **Certificación**: una solución basada en blockchain que garantiza la autenticidad del contenido compartido.
- **SPLA de Cyber Infrastructure**

En el portal de administración, puede seleccionar qué servicios y conjuntos de características estarán disponibles para sus inquilinos. La configuración se realiza por inquilino cuando suministra o edita un inquilino, como se describe en Creación de un inquilino.

Modos de facturación para Cyber Protect

Un modo de facturación es un esquema de contabilidad y facturación por el uso de servicios y sus características. El modo de facturación determina qué unidades se utilizarán como base para el cálculo de precios. Los partners pueden configurar los modos de facturación a nivel del cliente.

El motor de licencias adquiere los elementos de oferta en función de las características necesarias de los planes de protección. Los usuarios pueden optimizar el nivel de protección y el coste mediante la personalización de sus planes de protección.

Nota
Solo puede utilizar un modo de facturación por inquilino de cliente.

Modos de facturación del componente Protección

Protección tiene dos modos de facturación:

- Por carga de trabajo
- Por gigabyte

El conjunto de características de ambos modos de facturación es idéntico.

En ambos modos de facturación, el servicio de protección incluye características de protección estándar que cubren la mayoría de los riesgos de ciberseguridad. Los usuarios pueden utilizarlas sin cargo adicional. Se contabilizará el uso de las características incluidas, pero no se facturará. Para ver una lista completa de los elementos de oferta incluidos y facturables, consulte "Servicios de Cyber Protect" (p. 7).

Aunque se haya activado un paquete Advanced para un cliente, la facturación solo empezará cuando el cliente comience a usar las características de dicho paquete en un plan de protección. Cuando se aplique una característica avanzada de un plan de protección, el motor de licencias asignará automáticamente la licencia necesaria a la carga de trabajo protegida.

Cuando se deja de utilizar una característica avanzada, la licencia se revoca y se detiene la facturación. El motor de licencias asigna automáticamente la licencia que refleja el uso real de las características.

Solo puede asignar licencias para las características del servicio estándar de Cyber Protect. Las características avanzadas se facturan según el uso y sus licencias no se pueden modificar de forma manual. El motor de licencias asigna y desasigna estas licencias automáticamente. Puede modificar el tipo de licencia para una carga de trabajo de forma manual, pero se reasignará cuando un usuario modifique el plan de protección para esa carga de trabajo.

Nota
La facturación para las características de protección avanzada no empieza cuando las activa. La facturación empieza cuando un cliente comienza a utilizar las características avanzadas en un plan de protección. Los conjuntos de características activadas se contarán y se incluirán en los informes de uso, pero no se facturarán a menos que se utilicen sus características.

Modos de facturación para File Sync & Share

File Sync & Share tiene los siguientes modos de facturación:

- Por usuario
- Por gigabyte

También puede aplicar las reglas de facturación de la edición heredada de File Sync & Share.

Nota
La facturación para File Sync & Share avanzado no empieza cuando lo activa. La facturación empieza cuando un cliente comienza a utilizar las características avanzadas. El conjunto de características avanzadas activadas se contará y se incluirán en los informes de uso, pero no se facturarán a menos que se utilicen sus características.

Facturación del envío de datos físicos

La facturación del envío de datos físicos sigue el modelo de pago por uso.

Facturación de certificación

La facturación de la certificación sigue el modelo de pago por uso.

Uso de los modelos de facturación con ediciones heredadas

Si todavía no ha migrado al modelo de facturación actual, utilice los elementos de oferta de uno de los modos de facturación para sustituir las ediciones heredadas. El motor de licencias optimizará automáticamente las licencias asignadas al cliente para minimizar la cantidad facturable.

Nota
No puede mezclar ediciones con modos de facturación.

Cambio desde las ediciones heredadas al modelo de licencias actual

Puede cambiar de forma manual los elementos de oferta para sus inquilinos mediante la edición de su perfil y la selección de elementos de oferta. Para obtener más información sobre el proceso de conmutación, consulte "Conmutación entre ediciones y modos de facturación" (p. 10).

Para cambiar de las ediciones a los modos de facturación para varios clientes, consulte Conmutador de la edición masiva para varios clientes (67942).

Conmutación entre ediciones y modos de facturación

En el portal de administración, puede modificar una cuenta de inquilino para cambiar elementos de oferta entre modos de facturación (pasar del modo por carga de trabajo a por gigabyte y viceversa) y entre ediciones heredadas y modos de facturación.

Para más información sobre la conmutación masiva de inquilinos, consulte Conmutador de la edición masiva para varios clientes (67942).

El proceso de conmutación incluye estos pasos.

1. Suministre los nuevos elementos de oferta a un inquilino de cliente (mediante la activación de elementos de oferta y la configuración de cuotas) para adaptarse a la funcionalidad que estaba disponible en el elemento de oferta original.
2. Anule la asignación a elementos de oferta que no se utilicen y asígnelos a cargas de trabajo según las características utilizadas en los planes de protección (reconciliación de uso).

La siguiente tabla ilustra el proceso en ambas direcciones.

	Dirección del conmutador	
	Edición > modos de facturación	**Modo de facturación > modo de facturación**
Conmutador de elementos de oferta	Active los elementos de oferta para cumplir con la funcionalidad que estaba disponible en la edición de origen.	Se activará el conjunto idéntico de elementos de oferta.
Conmutador de cuota	Se replicará la cuota del elemento de oferta de origen a los elementos de oferta de destino. Estándar de origen → producto estándar de destino. Estándar de origen → paquetes de destino. **Nota** Si lleva a cabo una conmutación desde una edición con subediciones (por ejemplo, "Cyber Protect [por carga de trabajo]"), las cuotas se resumirán.	Se replicarán las cuotas del elemento de oferta de origen al elemento de oferta de destino.

	Dirección del conmutador	
	Edición > modos de facturación	**Modo de facturación > modo de facturación**
Conmutador de uso	Los elementos de oferta se reasignarán a las cargas de trabajo según las características que requieran los planes de protección asignados a esas cargas de trabajo.	

Ejemplo: Pasos para cambiar de una edición Advanced de Cyber Protect a una facturación por carga de trabajo

En esta situación, un inquilino cliente utiliza la edición Cyber Protect Advanced en ocho estaciones de trabajo y la cuota se establece en 10 cargas de trabajo. Tres de las estaciones de trabajo utilizan un inventario de software y la gestión de parches en sus planes de protección, dos estaciones de trabajo tienen el filtro de URL activado en sus planes de protección y una de las máquinas utiliza una protección continua de datos. La siguiente tabla muestra la conversión de la edición a los nuevos elementos de oferta.

Elementos de oferta de origen: uso/cuota	Elementos de oferta de destino: uso/cuota
Cyber Protect Advanced Workstation 8/10	• Workstation: 8/10 • Seguridad avanzada: 2/10 • Advanced Backup Workstation: 1/10 • Administración avanzada: 3/10

Los siguientes pasos se llevan a cabo durante la conmutación:

1. Los elementos de oferta para cumplir con la funcionalidad que estaba disponible en la edición de origen se activan automáticamente.
2. Se replica la cuota en los nuevos elementos de oferta.
3. El uso se concilió de acuerdo con el uso real de los planes de protección: tres cargas de trabajo usan características del paquete de administración avanzada, dos usan características del paquete de seguridad avanzada y una usa características del paquete de copia de seguridad avanzada.

Ejemplo: de la edición de Cyber Protect por carga de trabajo al modo de facturación por carga de trabajo

En este ejemplo, el cliente tiene varias ediciones asignadas a cargas de trabajo. Cada carga de trabajo puede tener solo una edición o un modo de facturación asignado.

Elementos de oferta de origen: uso/cuota	Elementos de oferta de destino: uso/cuota
Cyber Protect Essentials Workstation: 6/12	• Workstation: 14/42 • Advanced Backup Workstation: 2/42 • Seguridad avanzada: 13/42

Elementos de oferta de origen: uso/cuota	Elementos de oferta de destino: uso/cuota
	• Administración avanzada: 5/42
Cyber Protect Standard Workstation: 5/10	
Cyber Protect Advanced Workstation: 2/10	
Cyber Backup Standard Workstation: 1/10	

Los siguientes pasos se llevan a cabo durante la conmutación:

1. Los elementos de oferta para cumplir con la funcionalidad que estaba disponible en todas las ediciones de origen se activan automáticamente. Con los modos de facturación, se pueden asignar varios elementos de oferta a una carga de trabajo según sea necesario.
2. Las cuotas se resumieron y se replicaron.
3. Se concilió el uso según los planes de protección.

Cambiar el modo de facturación de un inquilino partner

Pasos para cambiar el modo de facturación de un inquilino partner

1. En el portal de gestión, vaya a **Clientes**.
2. Seleccione el inquilino partner cuyo modo de facturación quiera cambiar, haga clic en el icono de puntos suspensivos y en **Configurar**.
3. En la pestaña **Cyber Protect**, seleccione el servicio para el que desee cambiar el modo de facturación y haga clic en **Editar**.
4. Seleccione el modo de facturación deseado y habilite o deshabilite los artículos de oferta disponibles según sea necesario.
5. Haga clic en **Guardar**.

Cambiar el modo de facturación de un inquilino cliente

Puede cambiar la facturación de un inquilino cliente de las siguientes maneras:

- Editando el modo de facturación original. Para hacerlo tiene que habilitar o deshabilitar artículos de oferta.
- Cambiándolo a un modo de facturación totalmente nuevo.

Para obtener más información sobre cómo editar los artículos de oferta disponibles, consulte Habilitar o deshabilitar artículos de oferta.

Pasos para cambiar el modo de facturación de un inquilino cliente

1. En el portal de gestión, vaya a **Clientes**.
2. Seleccione el inquilino cliente cuya edición quiera cambiar, haga clic en el icono de puntos suspensivos y luego en **Configurar**.

3. En la pestaña **Configurar**, debajo de **Servicio**, seleccione el nuevo modo de facturación.
   Aparece un cuadro de diálogo para informarle sobre las consecuencias de cambiar al nuevo modo de facturación.
4. Introduzca su nombre de usuario para confirmar su elección.

Nota
Este cambio puede tardar hasta 10 minutos en completarse.

Artículos de oferta y gestión de cuotas

Esta sección describe:

- ¿Qué son los servicios y los elementos de oferta?
- Cómo se habilitan o deshabilitan los artículos de oferta.
- ¿Qué son los modos de facturación?
- ¿Qué son los paquetes de protección avanzada?
- ¿Qué son las ediciones y las subediciones heredadas?
- Qué son las cuotas flexibles y rígidas.
- Cuándo se puede sobrepasar una cuota rígida.
- Qué es la transformación de cuotas de copias de seguridad.
- ¿Cómo afecta la disponibilidad del artículo de oferta a la disponibilidad del programa de instalación en la consola de servicio?

Servicios y elementos de oferta

Servicios

Un servicio en la nube es un conjunto de funcionalidades alojado por un partner o por la nube privada de un cliente final. Por lo general, los servicios se venden como una suscripción o según el modelo de pago por uso.

El servicio Cyber Protect integra la ciberseguridad, la gestión y la protección de datos para proteger endpoints, sistemas y datos de ciberamenazas. El servicio Cyber Protect consta de varios componentes: Protección, File Sync & Share, Certificación y envío de datos físicos. Algunos de ellos pueden ampliarse con la funcionalidad avanzada mediante el uso de paquetes de protección avanzada. Para más información acerca de las características incluidas y avanzadas, consulte "Servicios de Cyber Protect" (p. 7).

Artículos de oferta

Un elemento de oferta es un conjunto de características de servicio agrupadas por un tipo de carga de trabajo específico o funcionalidad, por ejemplo, almacenamiento, recuperación ante desastres o infraestructura, entre otros. Al activar elementos de oferta específicos, determina qué cargas de

trabajo se pueden proteger, cuántas pueden protegerse (mediante el establecimiento de cuotas) y el nivel de protección disponible para tus partners, clientes y sus usuarios finales (mediante la activación o desactivación de paquetes de protección avanzada).

Las funcionalidades que no se activen se ocultarán a los clientes y usuarios, a menos que configure un escenario de venta de productos de gama superior. Para obtener más información sobre los escenarios de venta de productos de gama superior, consulte "Configuración de situaciones relacionadas con la venta de productos de gama superior a sus clientes" (p. 68).

El uso de la función se recopila de los servicios y se refleja en los elementos de oferta, que se utiliza en los informes y en la facturación adicional.

Modos de facturación y ediciones

Con las ediciones heredadas, puede activar solo un elemento de oferta por carga de trabajo. Con los modos de facturación, la funcionalidad se divide, por lo que puede activar varios elementos de oferta (características de servicio y paquetes avanzados) por carga de trabajo para adaptarse mejor a las necesidades de sus clientes y aplicar una facturación más precisa, solo para las características que realmente utilizan sus clientes.

Para obtener más información sobre los modos de facturación para Cyber Protect, consulte "Modos de facturación para Cyber Protect" (p. 8).

Puede utilizar los modos de facturación o las ediciones para configurar los servicios disponibles para sus inquilinos. Puede seleccionar un modo de facturación o una edición por inquilino de cliente. Como resultado, necesitará crear varios inquilinos para un cliente para aplicar diferentes modos de facturación para distintas características de servicio. Por ejemplo, si el cliente quiere tener los buzones de correo de Microsoft 365 con un modo de facturación por gigabyte y Teams con un modo de facturación por carga de trabajo, debe crear dos inquilinos diferentes para ese cliente.

Para limitar el uso de los servicios de un elemento de oferta, puede definir cuotas para ese elemento. Consulte "Cuotas flexibles y rígidas" (p. 15).

Habilitar o deshabilitar artículos de oferta

Puede activar todos los elementos de oferta disponibles para una edición determinada o un modo de facturación, tal y como se describe en Creación de un inquilino.

Nota
Desactivar todos los elementos de oferta de un servicio no desactiva el servicio automáticamente.

Existen ciertas limitaciones para deshabilitar artículos de oferta, que se indican en la siguiente tabla.

Artículo de oferta	Deshabilitar	Resultado
Almacenamiento de copias de seguridad	Se puede deshabilitar cuando el uso es igual a cero.	El almacenamiento en el cloud estará disponible como destino de copias de seguridad dentro del inquilino de un cliente.

Copia de seguridad local	Se puede deshabilitar cuando el uso es igual a cero.	El almacenamiento local no estará disponible como destino de copias de seguridad dentro del inquilino de un cliente.
Orígenes de datos (incluidos Microsoft 365 y Google Workspace)	Se puede deshabilitar cuando el uso es igual a cero.	La copia de seguridad y la recuperación de orígenes de datos (incluidos Microsoft 365 y Google Workspace) no estarán disponibles en el inquilino de un cliente.
Todos los artículos de oferta de recuperación ante desastres	Se puede deshabilitar cuando el uso es mayor que cero.	Consulte los detalles en "Cuotas flexibles y rígidas".
Todos los artículos de oferta de certificación	Se puede deshabilitar cuando el uso es igual a cero.	El servicio de certificación no estará disponible en el inquilino de un cliente.
Todos los artículos de oferta de File Sync & Share	No es posible habilitar o deshabilitar por separado los artículos de oferta.	El servicio de File Sync & Share no estará disponible en el inquilino de un cliente.
Todos los artículos de oferta de envío de datos físicos	Se puede deshabilitar cuando el uso es igual a cero.	El servicio de envío de datos físicos no estará disponible en el inquilino de un cliente.

Si un artículo de oferta no se puede deshabilitar cuando su uso es mayor que cero, puede eliminar el uso manualmente y después deshabilitar el artículo de oferta correspondiente.

Cuotas flexibles y rígidas

Las **cuotas** le permiten limitar la capacidad de los inquilinos de utilizar el servicio. Para establecer las cuotas, seleccione el Cliente en la pestaña **Clientes**, seleccione la pestaña de servicio y haga clic en **Editar**.

Cuando se supera una cuota, se envía una notificación a la dirección de correo electrónico del usuario. Si no establece un uso por encima del límite de cuota, la cuota se considera "**flexible**". Esto significa que no se aplican restricciones para usar el servicio de Cyber Protection.

Al especificar el uso por encima del límite de cuota, esta se considera "**rígida**". Un **uso por encima del límite** permite al usuario sobrepasar la cuota en un valor especificado. Si el uso por encima del límite se sobrepasa, se aplican las restricciones sobre el uso del servicio.

Ejemplo

Cuota flexible: Ha establecido el valor 20 para la cuota de estaciones de trabajo. Cuando se llegue a las 20 estaciones de trabajo protegidas, el cliente recibirá una notificación por correo electrónico, pero el servicio Cyber Protection seguirá estando disponible.

Cuota rígida: Si ha establecido la cuota de estaciones de trabajo en 20 y el exceso admitido es de 5, el cliente recibirá la notificación por correo electrónico cuando llegue a 20 estaciones de trabajo protegidas, y el servicio Cyber Protection se deshabilitará cuando alcance las 25.

Cuando se alcanza una cuota estricta, el servicio se limita (no se puede proteger otra carga de trabajo o utilizar más almacenamiento). Cuando se supera la cuota estricta, se envía una notificación a la dirección de correo electrónico del usuario.

Niveles en los que se pueden definir las cuotas

Las cuotas se pueden establecer en los niveles que aparecen en la siguiente tabla.

Inquilino/Usuario	Cuota flexible (solo cuota)	Cuota rígida (cuota y uso por encima del límite)
Socio	sí	no
Carpeta	sí	no
Cliente	sí	sí
Unidad	no	no
Usuario	sí	sí

Las cuotas flexibles se pueden establecer en los niveles de carpeta y socio. No se pueden establecer cuotas en el nivel de unidad. Las cuotas rígidas se pueden establecer en los niveles de cliente y usuario.

La cantidad total de cuotas rígidas que se establecen en el nivel de usuario no puede sobrepasar la cuota rígida del cliente relacionada.

Configuración de cuotas flexibles y estrictas

Configuración de cuotas para sus clientes

1. En el portal de gestión, vaya a **Clientes**.
2. Seleccione el cliente para el que desea configurar cuotas.
3. Seleccione la pestaña **Protección** y, a continuación, haga clic en **Editar**.
4. Seleccione el tipo de cuota que desea establecer. Por ejemplo, seleccione **Estaciones de trabajo** o **Servidores**.
5. Haga clic en el enlace **Ilimitado** a la derecha para abrir la ventana **Edición de la cuota**.
   - Si quiere informar al cliente de la cuota sin limitar su capacidad de usar el servicio, establezca el valor de la cuota en el campo **Cuota flexible**.
     El cliente recibirá una notificación por correo electrónico al alcanzar la cuota, pero el servicio de Cyber Protection seguirá disponible.
   - Si quiere limitar la capacidad del cliente de usar el servicio, seleccione **Cuota estricta** y establezca el valor de la cuota en el campo debajo de **Cuota estricta**.

El cliente recibirá una notificación por correo electrónico al alcanzar la cuota y el servicio de Cyber Protection se deshabilitará.

6. En la ventana **Edición de la cuota**, haga clic en **Listo** y, a continuación, en **Guardar**.

Cuotas de Backup

Puede especificar la cuota de almacenamiento en el cloud, la de copia de seguridad local y el número máximo de equipos, dispositivos o sitios web que un usuario puede proteger. Están disponibles las siguientes cuotas.

Cuota de dispositivos

- **Estaciones de trabajo**
- **Servidores**
- **Equipos virtuales**
- **Dispositivos móviles**
- **Servidores de alojamiento web** (servidores físicos y virtuales basados en Linux que ejecuten paneles de control Plesk, cPanel, DirectAdmin, VirtualMin o ISPManager)
- **Sitios web**

Se considera que un equipo, un dispositivo o un sitio web están protegidos si se les aplica, como mínimo, un plan de protección. Un dispositivo móvil se considera protegido después de la primera copia de seguridad.

Cuando se supera el límite de exceso de dispositivos, el usuario no puede aplicar un plan de protección a más dispositivos.

Cuotas de orígenes de datos en el cloud

- **Licencias de Microsoft 365**
  Esta cuota la aplica el proveedor de servicios a toda la empresa. Los administradores de la empresa pueden ver la cuota y el uso en el portal de gestión.
  La concesión de licencias de usuarios de Microsoft 365 depende del modo de facturación seleccionado para Cyber Protection.
  En el modo de facturación **por carga de trabajo**, la cuota de **licencias de Microsoft 365** se cuenta por usuarios únicos. Un usuario único es un usuario que tiene, al menos, uno de los siguientes:
  - Buzón de correo protegido
  - OneDrive protegido
  - Acceso a, como mínimo, un recurso de nivel de empresa protegido: Un sitio de Microsoft 365 SharePoint Online o Microsoft 365 Teams.
    Para comprobar el número de miembros de un sitio de Microsoft 365 SharePoint o Teams, consulte este artículo de la base de conocimientos.

Nota

No se cobra a los usuarios bloqueados de Microsoft 365 que no tienen un buzón de correo personal protegido o OneDrive, y solo pueden acceder a recursos compartidos (buzones de correo compartidos, sitios de SharePoint y Microsoft Teams).

Los usuarios bloqueados son aquellos que no tienen un inicio de sesión válido y no pueden acceder a los servicios de Microsoft 365. Para aprender a bloquear a todos los usuarios sin licencia en una organización de Microsoft 365, consulte "Impedir que los usuarios de Microsoft 365 sin licencia inicien sesión" (p. 20).)

No se le cobrará por los siguientes usuarios de Microsoft 365 y no requieren una licencia por usuario:

- Buzones de correo compartidos
- Salas y equipos
- Usuarios externos con acceso a sitios de SharePoint o Microsoft Teams con copia de seguridad

Para obtener más información sobre las opciones de licencia con el modo de facturación por gigabyte, consulte Cyber Protect Cloud: Licencias de Microsoft 365 por GB.

Para obtener más información sobre las opciones de licencia con el modo de facturación por carga de trabajo, consulte Cyber Protect Cloud: Licencias de Microsoft 365 y cambios de precios.

- **Microsoft 365 Teams**

  Esta cuota la aplica el proveedor de servicios a toda la empresa. Esta cuota habilita o deshabilita la capacidad de proteger Microsoft 365 Teams y establece el número máximo de equipos que es posible proteger. Para proteger un equipo, independientemente de su número de miembros o canales, se necesita una cuota. Los administradores de la empresa pueden ver la cuota y el uso en el portal de gestión.

- **Microsoft 365 SharePoint Online**

  Esta cuota la aplica el proveedor de servicios a toda la empresa. Esta cuota habilita o deshabilita la capacidad de proteger SharePoint Online y establece el número máximo de recopilaciones de sitios y grupos de sitios que es posible proteger.

  Los administradores de la empresa pueden ver la cuota y el uso en el portal de administración. También pueden ver la cuota junto con la cantidad de almacenamiento que ocupan las copias de seguridad de SharePoint Online en los informes de uso.

- **Licencias de Google Workspace**

  Esta cuota la aplica el proveedor de servicios a toda la empresa. Se puede permitir que la empresa proteja buzones de correo de **Gmail** (incluido Calendar y Contactos), archivos de **Google Drive** o ambos. Los administradores de la empresa pueden ver la cuota y el uso en el portal de gestión.

- **Unidad compartida de Google Workspace**

  Esta cuota la aplica el proveedor de servicios a toda la empresa. Esta cuota habilita o deshabilita la capacidad de proteger unidades compartidas de Google Workspace. Si la cuota está habilitada, se pueden proteger todas las unidades compartidas que se desee. Los administradores de la

empresa no pueden ver la cuota en el portal de gestión, pero sí la cantidad de almacenamiento ocupado por copias de seguridad de unidades compartidas en los informes de uso.

La realización de copias de seguridad de unidades compartidas de Google Workspace solo está disponible para clientes que también tengan una cuota de puestos de Google Workspace como mínimo. Esta cuota solo se verificará, así que el proceso no tardará.

Se considera que una licencia de Microsoft 365 está protegida si se ha aplicado, como mínimo, un plan de protección al buzón de correo o al OneDrive del usuario. Se considera que una licencia de Google Workspace está protegida si se ha aplicado, como mínimo, un plan de protección al buzón de correo o al Google Drive del usuario.

Si se supera el límite de exceso de licencias, el administrador de una empresa no puede aplicar un plan de protección a más licencias.

Cuotas de almacenamiento

- **Copia de seguridad local**

  La cuota de las **copias de seguridad locales** limita el tamaño total de las copias de seguridad locales que se crean mediante el uso de la infraestructura en la cloud. Para esta cuota no se puede establecer un uso por encima del límite.
- **Recursos en el cloud**

  La cuota de **recursos en el cloud** combina la cuota del almacenamiento de copias de seguridad y las de recuperación ante desastres. La cuota de almacenamiento de copias de seguridad limita el tamaño total de las copias de seguridad que se encuentran en el almacenamiento en el cloud. Si se supera este uso por encima del límite de la cuota de almacenamiento de copias de seguridad, no se realizan copias de seguridad.

Rebasamiento de la cuota de almacenamiento de copias de seguridad

No se puede exceder la cuota de almacenamiento de copias de seguridad. El certificado del agente de protección tiene una cuota técnica que equivale a la cuota de copia de seguridad del inquilino + el exceso. No se puede iniciar una copia de seguridad si se ha excedido la cuota. Si la cuota del certificado se alcanza durante la creación de la copia de seguridad pero no se alcanza el exceso, la copia de seguridad se completará con éxito. Si se alcanza el exceso durante la creación de la copia de seguridad, esta fallará.

Ejemplo:

Un inquilino de usuario tiene 1 TB de espacio libre de cuota y el exceso configurado para dicho usuario es de 5 TB. El usuario inicia una copia de seguridad. Si el tamaño de la copia de seguridad creada es, por ejemplo, 3 TB, la copia de seguridad se completará con éxito porque el exceso no se ha rebasado. Si el tamaño de la copia de seguridad creada es, por ejemplo, mayor que 6 TB, la copia de seguridad fallará cuando se supere el exceso.

Transformación de la cuota de copia de seguridad

En general, así es como se adquiere una cuota de copia de seguridad y se asignan artículos de oferta a tipos de recursos: el sistema compara los artículos de oferta disponibles con el tipo de recurso y después adquiere la cuota para el artículo de oferta coincidente.

También es posible asignar otra cuota a un artículo de oferta aunque no coincida totalmente con el tipo de recurso. Esto se denomina **transformación de la cuota de copia de seguridad**. Si no hay un artículo de oferta coincidente, el sistema busca una cuota mayor y más apropiada para el tipo de recurso (transformación automática de la cuota de copia de seguridad). Si no se encuentra nada adecuado, puede asignar la cuota de servicio manualmente al tipo de recurso en la consola de servicio.

Ejemplo

Quiere realizar una copia de seguridad de un equipo virtual (una estación de trabajo basada en agentes).

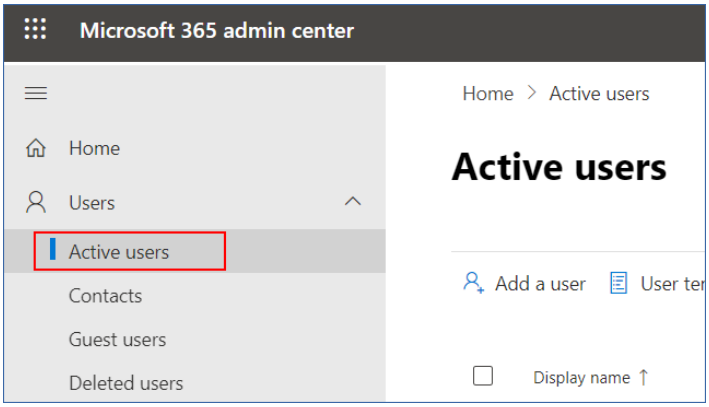
Primero, el sistema comprobará si hay una cuota asignada a **equipos virtuales**. Si no la encuentra, el sistema intentará adquirir automáticamente la cuota de **estaciones de trabajo**. Si tampoco la encuentra, no se adquirirá automáticamente la otra cuota. Si cuenta con una cuota suficiente que sea más costosa que la de los **equipos virtuales** y se pueda aplicar a un equipo virtual, puede iniciar sesión en la consola de servicio y asignar la cuota a los **servidores** manualmente.

Impedir que los usuarios de Microsoft 365 sin licencia inicien sesión

Para impedir que todos los usuarios sin licencia en la organización de Microsoft 365 inicien sesión, puede modificar su estado de inicio de sesión.

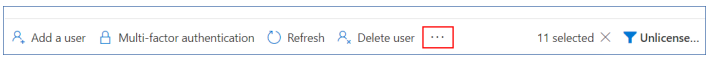
Para impedir que los usuarios sin licencia inicien sesión

1. Inicie sesión en el Centro de administración de Microsoft 365 (https://admin.microsoft.com) como administrador global.
2. En el menú de navegación, vaya a **Usuarios** > **Usuarios activos**.



3. Haga clic en **Filtro** y seleccione **Usuarios sin licencia**.

4. Seleccione las casillas de verificación que se encuentran junto a los nombres de usuario y después haga clic en el icono de puntos suspensivos (...).



5. En el menú, seleccione **Editar estado de inicio de sesión**.
6. Seleccione la casilla de verificación **Impedir que los usuarios inicien sesión** y haga clic en **Guardar**.

Cuotas de Disaster Recovery

Nota
Los artículos de oferta de recuperación ante desastres solo están disponibles con el complemento de recuperación ante desastres.

Estas cuotas las aplica el proveedor de servicios a toda la empresa. Los administradores de la empresa pueden ver las cuotas y el uso en el portal de gestión, pero no pueden establecer cuotas para un usuario.

- **Almacenamiento de recuperación ante desastres**
  El almacenamiento de la recuperación ante desastres muestra el tamaño del almacenamiento inactivo de los servidores protegidos por la recuperación ante desastres. Este almacenamiento se calcula a partir de la hora en la que se crea el servidor de recuperación, independientemente de si el servidor se está ejecutando actualmente o no. Si se alcanza el uso por encima del límite para esta cuota, no se podrán crear servidores principales ni de recuperación ni agregar o extender discos de los servidores principales existentes. Si se supera el uso por encima del límite para esta cuota, no se podrá iniciar una conmutación por error ni simplemente iniciar un servidor detenido. Los servidores en ejecución siguen funcionando.
- **Puntos del equipo**
  Esta cuota limita los recursos de la CPU y la RAM que consumen los servidores principales y los de recuperación durante un periodo de facturación. Si se alcanza el uso por encima del límite para esta cuota, todos los servidores principales y de recuperación se apagarán. Estos servidores no se pueden usar hasta que comience el siguiente periodo de facturación. El periodo de facturación predeterminado es un mes completo.
  Cuando la cuota se deshabilita, los servidores no se pueden usar, independientemente del periodo de facturación.
- **Direcciones IP públicas**
  Esta cuota limita el número de direcciones IP públicas que se pueden asignar a los servidores principales y de recuperación. Si se alcanza el uso por encima del límite para esta cuota, no se podrán habilitar direcciones IP públicas para más servidores. Desmarque la casilla de verificación **Dirección IP pública** de la configuración del servidor para hacer que no pueda usar ninguna IP pública. Después, puede permitir que otro servidor use una dirección IP pública, que normalmente no será la misma.

Cuando la cuota se deshabilita, todos los servidores dejan de usar direcciones IP públicas y, por tanto, no se puede acceder a ellos desde Internet.

- **Servidores en la cloud**

  Esta cuota limita el número total de servidores primarios y de recuperación. Si se alcanza el uso por encima del límite para esta cuota, no se podrán crear servidores principales ni de recuperación.

  Cuando la cuota se deshabilita, los servidores se pueden ver en la consola de servicio, pero la única operación disponible es **Eliminar**.
- **Acceso a Internet**

  Esta cuota habilita o deshabilita el acceso a Internet desde servidores principales y de recuperación.

  Cuando la cuota está deshabilitada, los servidores principales y de recuperación no pueden establecer conexión a Internet.

Cuotas de File Sync & Share

Puede definir las siguientes cuotas de File Sync & Share para un inquilino:

- **Usuarios**

  La cuota define el número de usuarios que pueden acceder a este servicio.

  Las cuentas de administrador no se incluyen como parte de esta cuota.
- **Almacenamiento en la cloud**

  Se trata de un almacenamiento en el cloud que permite guardar los archivos de los usuarios. La cuota define el espacio asignado a un inquilino en el almacenamiento en el cloud.

Cuotas de envío de datos físicos

Las cuotas del servicio de envío de datos físicos se consumen por unidad. Puede guardar copias de seguridad iniciales de múltiples equipos en una unidad de disco rígido.

Puede definir las siguientes cuotas de envío de datos físicos para un inquilino:

- **En el cloud**

  Permite enviar una copia de seguridad inicial al centro de datos en el cloud con una unidad de disco rígido. Esta cuota define el número máximo de unidades que se pueden transferir al centro de datos en la nube.

Cuotas de certificación

Puede definir las siguientes cuotas de certificación para un inquilino:

- **Almacenamiento de Notary**

  El almacenamiento de Notary es el almacenamiento en la nube donde se guardan los archivos certificados ante notario, los firmados y aquellos cuya certificación está en progreso. Esta cuota define el espacio máximo que pueden ocupar estos archivos.

Para reducir el uso de esta cuota, puede eliminar los archivos ya certificados ante notario o firmados del almacenamiento de Notary.

- **Notarizaciones**

  Esta cuota define el número máximo de archivos que se pueden certificar ante notario con el servicio de certificación. Un archivo se considera certificado ante notario en el momento en el que se carga al almacenamiento de Notary y su estado de certificación cambia a En progreso.

  Si el mismo archivo se certifica varias veces, cada certificación cuenta como una nueva.
- **Firmas electrónicas**

  Esta cuota define el número máximo de archivos que se pueden firmar con el servicio de certificación. Un archivo se considera firmado desde el momento en el que se envía para su firma.

Cambiar la cuota de servicio de equipos

El nivel de protección de un equipo se define por la cuota de servicio aplicada. Las cuotas de servicio están relacionadas con los artículos de oferta disponibles para el inquilino en el que está registrado el equipo.

Una cuota de servicio se asigna automáticamente cuando se aplica un plan de protección a un equipo por primera vez.

Se asigna la cuota más apropiada, según el tipo de equipo protegido, su sistema operativo, el nivel de protección requerido y la disponibilidad de la cuota. Si la cuota más adecuada no está disponible en su organización, se asignará la segunda mejor cuota. Por ejemplo, si la cuota más adecuada es **Servidor de alojamiento web**, pero no está disponible, se asignará la cuota **Servidor**.

Ejemplos de asignación de cuotas:

- A un equipo físico que ejecuta un sistema operativo Windows Server o Linux se le asigna la cuota **Servidor**.
- A un equipo físico que ejecuta un sistema operativo Windows de escritorio se le asigna la cuota **Estación de trabajo**.
- A un equipo físico que ejecuta Windows 10 con el rol Hyper-V habilitado se le asigna la cuota **Estación de trabajo**.
- A un equipo de escritorio que se ejecuta en una infraestructura de escritorio virtual y cuyo agente de protección se instala dentro del sistema operativo invitado (por ejemplo, Agente para Windows) se le asigna la cuota **Máquina virtual**. Este tipo de equipo también puede utilizar la cuota **Estación de trabajo** si la cuota **Máquina virtual** no está disponible.
- A un equipo de escritorio que se ejecuta en una infraestructura de escritorio virtual y de cuyo agente se hace una copia de seguridad en el modo sin agente (por ejemplo, por Agente para VMware o Agente para Hyper-V) se le asigna la cuota **Máquina virtual**.
- A un servidor Hyper-V o vSphere se le asigna la cuota **Servidor**.
- A un servidor con cPanel o Plesk se le asigna la cuota **Servidor de alojamiento web**. También puede utilizar la cuota **Máquina virtual** o la cuota **Servidor**, según el tipo de equipo en el que se ejecute el servidor web, si la cuota **Servidor de alojamiento web** no está disponible.

- La copia de seguridad con información de aplicaciones requiere la cuota **Servidor**, incluso para una estación de trabajo.

Puede cambiar manualmente la asignación original más adelante. Por ejemplo, para aplicar un plan de protección más avanzado al mismo equipo, es posible que tenga que mejorar la cuota de servicio del mismo. Si las características que necesita este plan de protección no son compatibles con la cuota de servicio asignada en ese momento, el plan de protección fallará.

Otra posibilidad es cambiar la cuota de servicio si adquiere una cuota más apropiada después de haber asignado la original. Por ejemplo, a una máquina virtual se le asigna la cuota **Estación de trabajo**. Después de adquirir una cuota de **Máquinas virtuales**, puede asignarla manualmente al equipo en lugar de la cuota **Estación de trabajo** original.

También puede liberar la cuota de servicio asignada actualmente para asignarla a otro equipo.

Puede cambiar la cuota de servicio de un equipo individual o de un grupo de equipos.

Pasos para cambiar la cuota de servicio de un equipo individual

1. En la consola de servicio de Cyber Protection, vaya a **Dispositivos**.
2. Seleccione el equipo que desee y haga clic en **Detalles**.
3. En la sección **Cuota de servicio**, haga clic en **Cambiar**.
4. En la ventana **Cambiar licencia**, seleccione la cuota de servicio que desee o **Sin cuota** y haga clic en **Cambiar**.

Pasos para cambiar la cuota de servicio de un grupo de equipos

1. En la consola de servicio de Cyber Protection, vaya a **Dispositivos**.
2. Seleccione más de un equipo y haga clic en **Asignar cuota**.
3. En la ventana **Cambiar licencia**, seleccione la cuota de servicio que desee o **Sin cuota** y haga clic en **Cambiar**.

Dependencia de instalador de agente para artículos de oferta

Dependiendo de los artículos de oferta permitidos, el programa de instalación de agente que corresponda estará disponible en la sección **Añadir dispositivos** de la consola de servicio. En la siguiente tabla, puede ver los programas de instalación de agentes y su disponibilidad en la consola de servicio en función de los artículos de oferta habilitados.

Artículo de oferta habilitado **Instalador del agente**	**Servidores**	**Estaciones de trabajo**	**Equipos virtuales**	**Usuarios de Microsoft 365**	**Licencias de Google Workspace**	**Dispositivos móviles**	**Servidores de alojamiento web**	**Sitios web**
Estaciones de trabajo:		+	+					+

agente para Windows								
Estaciones de trabajo: agente para Mac OS		+	+					+
Servidores: agente para Windows	+		+				+	+
Servidores: agente para Linux	+		+				+	+
Agente para Hyper-V			+					
Agente para VMware			+					
Agente para Virtuozzo			+					
Agente para SQL	+		+					
Agent for Exchange	+		+					
Agente para Active Directory	+		+					
Agente para Microsoft 365				+				
Agente para Google Workspace					+			
Instalador completo para Windows	+	+	+				+	+
Móvil (iOS y Android)						+		

Uso del portal de gestión

Los siguientes pasos lo guiarán a través del uso básico del portal de gestión.

Navegadores web compatibles

La interfaz web es compatible con los siguientes navegadores web:

- Google Chrome 29 o posterior
- Mozilla Firefox 23 o posterior
- Opera 16 o posterior
- Microsoft Edge 25 o posterior
- Safari 8 o una versión posterior que se ejecute en los sistemas operativos macOS y iOS

En otros navegadores web (incluido Safari para otros sistemas operativos), es posible que la interfaz de usuario no se muestre correctamente o que algunas funciones no estén disponibles.

Activación de la cuenta de administrador.

Tras firmar el acuerdo de colaboración, recibirá un correo electrónico con la siguiente información:

- **Sus credenciales de inicio de sesión.** Este es el nombre de usuario que utiliza para iniciar sesión. Sus credenciales de inicio de sesión aparecen también en la página de activación de la cuenta.
- Botón **Activar cuenta**. Haga clic en el botón y establezca la contraseña de su cuenta. Asegúrese de que la contraseña tenga al menos nueve caracteres. Para obtener más información sobre la contraseña, consulte "Requisitos de contraseña" (p. 26).

Requisitos de contraseña

La contraseña de las cuentas de usuario debe tener una longitud de al menos 9 caracteres. También se comprueba la complejidad de las contraseñas, que entran dentro de una de las siguientes categorías:

- Débil
- Medio
- Fuerte

No puede guardar una contraseña débil, incluso aunque contenga 9 caracteres o más. Las contraseñas que repiten el nombre de usuario, el inicio de sesión, el correo electrónico del usuario o el nombre del inquilino al que pertenece la cuenta de usuario siempre se consideran débiles. Las contraseñas más comunes también se consideran débiles.

Para reforzar una contraseña, añada más caracteres. No es obligatorio utilizar diferentes tipos de caracteres, como números, mayúsculas y minúsculas y caracteres especiales, pero se obtienen contraseñas más fuertes y más cortas.

Acceso al portal de gestión

1. Vaya a la página de inicio de sesión del servicio.
   La dirección de la página de inicio de sesión se incluye en el correo electrónico de activación que ha recibido.
2. Escriba el usuario y haga clic en **Siguiente**.
3. Escriba la contraseña y haga clic en **Siguiente**.

   Nota
   Para proteger Cyber Protect Cloud de ataques de fuerza bruta, el portal le bloqueará tras 10 intentos de inicio de sesión fallidos. El período de bloqueo es de 5 minutos. El número de intentos de inicio de sesión fallidos se restablece tras 15 minutos.

4. Utilice el menú de la derecha para navegar por el portal de administración.

El tiempo de espera para el portal de administración es de 24 horas en las sesiones activas y de 1 hora en las inactivas.

Algunos servicios incluyen la capacidad de cambiar al portal de gestión desde la consola del servicio.

Configuración de contactos en el asistente de Perfil de empresa

Puede configurar la información de contacto de su empresa. Enviaremos actualizaciones sobre las nuevas características y otros cambios importantes de la plataforma a los contactos que proporcione.

Cuando inicie sesión en el portal de administración por primera vez, el asistente de Perfil de empresa le guiará por la información básica sobre la empresa y los contactos que debe proporcionar.

Puede crear contactos de usuarios que existan en la plataforma de Cyber Protect o añadir la información de contacto de las personas que no tengan acceso al servicio.

Configurar contactos con el asistente de Perfil de empresa

1. En **Información de la empresa**, especifique los siguientes detalles de su empresa:
   - **Nombre oficial (legal) de la empresa**
   - **Dirección legal de la empresa (dirección de la sede central)**
     - **País**
     - **Código postal**

2. Haga clic en **Siguiente**.
3. En **Contactos de la empresa**, configure los contactos para los siguientes fines:
   - **Contacto de facturación**: el contacto que obtendrá información sobre los cambios importantes que se produzcan en la creación de informes de uso en la plataforma.
   - **Contacto empresarial**: el contacto que recibirá actualizaciones sobre cambios comerciales importantes en la plataforma.
   - **Contacto técnico**: el contacto que recibirá actualizaciones sobre cambios técnicos importantes en la plataforma.

   Puede usar un contacto para más de un fin.

   Seleccione una opción para crear el contacto.
   - **Crear a partir de un usuario existente**. Seleccione un usuario de la lista desplegable.
   - **Crear un contacto nuevo**. Proporcione la siguiente información de contacto:
     - **Nombre**: nombre de la persona de contacto. Este campo es obligatorio.
     - **Apellidos**: apellidos de la persona de contacto. Este campo es obligatorio.
     - **Dirección de correo electrónico de empresa**: dirección de correo electrónico de la persona de contacto. Este campo es obligatorio.
     - **Teléfono del trabajo**: este campo es opcional.
     - **Puesto**: este campo es opcional.
4. Si tiene pensado utilizar el contacto de facturación como contacto empresarial y técnico, seleccione las marcas correspondientes en la sección **Contacto de facturación**:
   - **Utilizar el mismo contacto para Contacto empresarial**
   - **Utilizar el mismo contacto para Contacto técnico**
5. Haga clic en **Realizado**.

   Como resultado, se han creado los contactos. Puede editar la información y configurar otros contactos en la sección **Gestión empresarial > Perfil de empresa** de la consola de administración, como se describe en Configuración de los contactos de la empresa.

Acceso a la consola de Cyber Protection desde el portal de administración

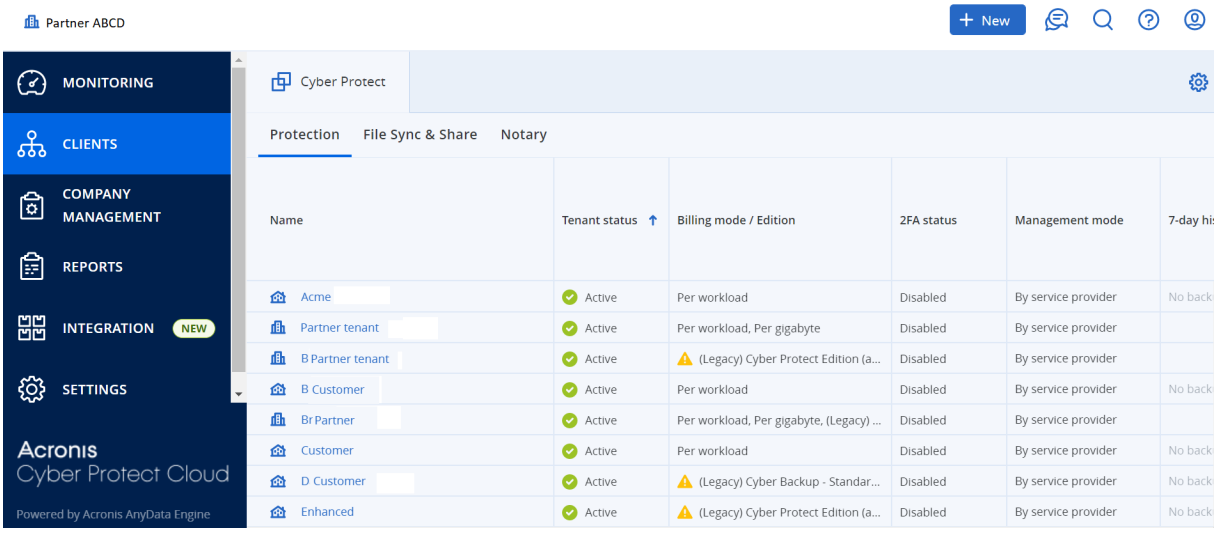
1. En el portal de administración, vaya a **Supervisión** > **Uso**.
2. En **Ciberprotección**, seleccione **Protección** y haga clic en **Gestionar servicio**.
   De manera alternativa, en **Clientes**, seleccione un cliente y haga clic en **Gestionar servicio**.

Como resultado, se le dirigirá a la consola de Cyber Protection.

Navegación en el portal de gestión

Cuando se utiliza el portal de gestión, en un momento dado está operando en un inquilino. El nombre de este inquilino se indica en la esquina superior izquierda.

De forma predeterminada, aparece seleccionado el máximo nivel de jerarquía disponible para usted. Haga clic en un nombre de inquilino de la lista para profundizar en la jerarquía. Para volver a un nivel superior, haga clic en su nombre en la esquina superior izquierda.



Todas las partes de la interfaz de usuario solo muestran y afectan al inquilino en que está operando actualmente. Por ejemplo:

- La pestaña **Clientes** solo muestra los inquilinos que son secundarios directos del inquilino en que está operando actualmente.
- La pestaña **Gestión empresarial** muestra el perfil de la empresa y las cuentas de usuario que existen en el inquilino en que está operando actualmente.
- Con el botón **Nuevo** puede crear un inquilino o una cuenta de usuario nueva únicamente en el inquilino en que está operando actualmente.

Limitación del acceso a la interfaz web

Los administradores pueden limitar el acceso a la interfaz web especificando una lista de direcciones IP desde las que los miembros de un inquilino pueden iniciar sesión.

Esta restricción también se aplica al acceso al portal de gestión a través de la API.

Esta restricción solo se aplica al nivel donde está configurado. Esta restricción *no* se aplica a los miembros de los inquilinos secundarios.

Para limitar el acceso a la interfaz web

1. Inicie sesión en el portal de gestión.
2. Vaya hasta el inquilino en el que desee limitar el acceso.
3. Haga clic en **Ajustes** > **Seguridad**.
4. Habilite el conmutador **Control de inicio de sesión**.
5. En **Direcciones IP permitidas**, indique las direcciones IP que quiere permitir.
   Puede escribir cualquiera de los parámetros siguientes separados por punto y coma.
   - Direcciones IP, por ejemplo: 192.0.2.0
   - Rangos de IP, por ejemplo: 192.0.2.0-192.0.2.255
   - Subredes, por ejemplo: 192.0.2.0/24
6. Haga clic en **Guardar**.

Nota
Para proveedores de servicio que utilizan Cyber Infrastructure (modelo híbrido):

Si el conmutador **Control de inicio de sesión** está habilitado en **Configuración** > **Seguridad** en el portal de administración, añada la dirección o direcciones IP públicas externas de los nodos de Cyber Infrastructure a la lista **Direcciones IP permitidas**.

Acceso a los servicios

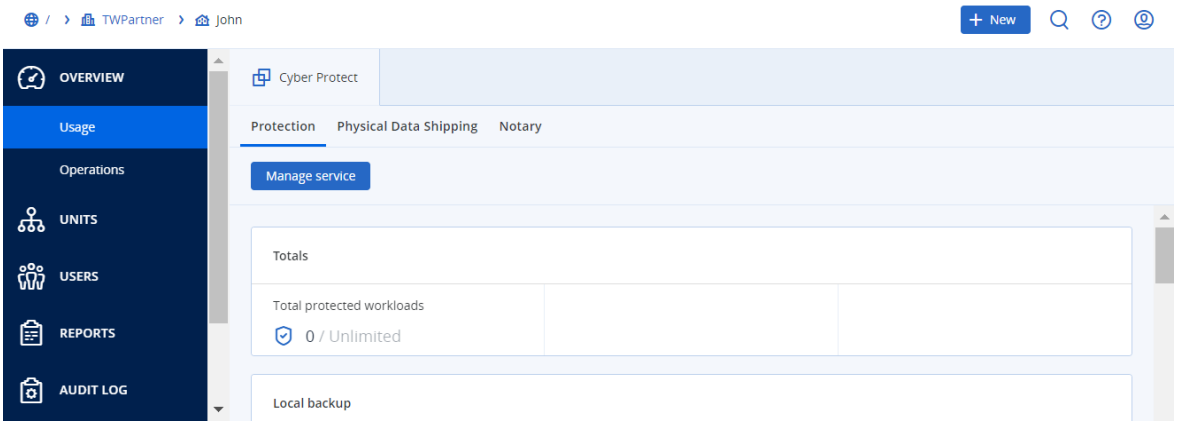
Pestaña General

En la sección **General** > **Uso** se ofrece un resumen del uso del servicio y a través de ella se puede acceder a los servicios del inquilino en el que está operando.

Pasos para gestionar un servicio para un inquilino con la pestaña General

1. Vaya hasta el inquilino en el que desee gestionar un servicio y, a continuación, haga clic en **General** > **Uso**.
   Tenga en cuenta que algunos servicios pueden gestionarse en el inquilino socio y en los niveles del inquilino cliente, mientras que otros servicios solo pueden gestionarse en el nivel del inquilino cliente.
2. Haga clic en el nombre del servicio que desea gestionar y, a continuación, haga clic en **Gestionar servicio** o en **Configurar servicio**.
   Para obtener más información sobre el uso de los servicios, consulte los manuales de usuario

disponibles en las consolas de servicio.

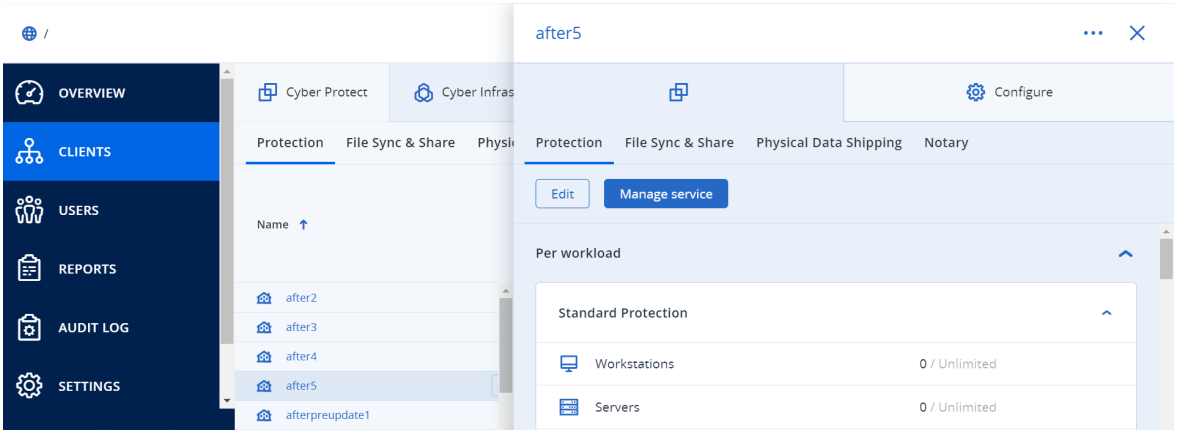


Pestaña Clientes

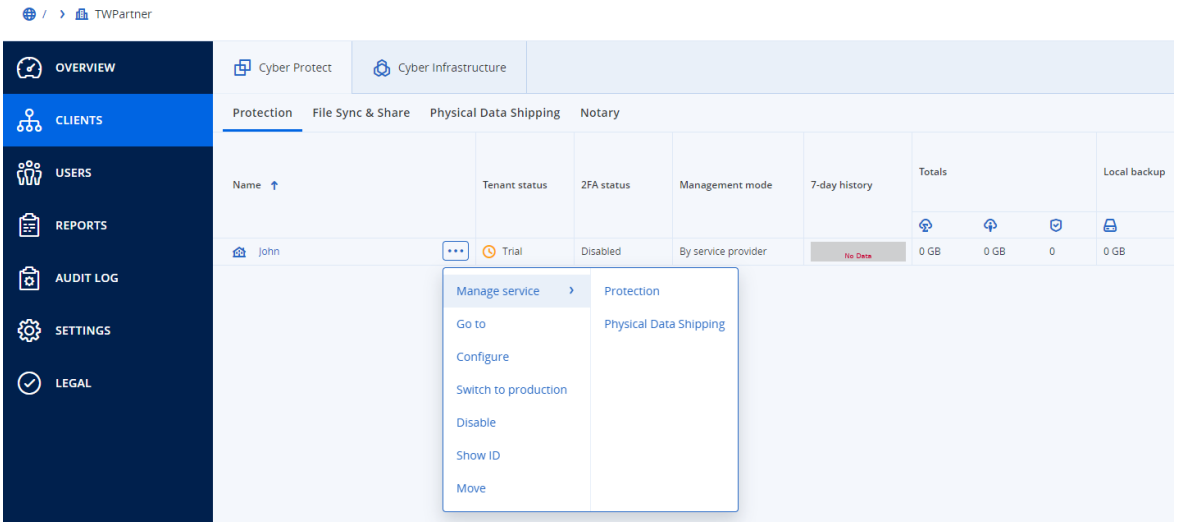
En la pestaña **Clientes** se muestran los inquilinos secundarios del inquilino en el que está operando y se permite acceder a los servicios que contienen.

Pasos para gestionar un servicio para un inquilino con la pestaña Clientes

1. Realice uno de los siguientes procedimientos:
   - Haga clic en **Clientes**, seleccione el inquilino en el que desee gestionar el servicio, después, haga clic en el nombre o el icono del servicio que desea gestionar y, a continuación, en **Gestionar servicio** o **Configurar servicio**.



   - Haga clic en **Clientes**, haga clic en en el icono de puntos suspensivos que se encuentra junto al nombre del inquilino y seleccione **Gestionar servicio**. Por último, seleccione el servicio que quiera gestionar.



Tenga en cuenta que algunos servicios pueden gestionarse en el inquilino socio y en los niveles del inquilino cliente, mientras que otros servicios solo pueden gestionarse en el nivel del inquilino cliente.

Para obtener más información sobre el uso de los servicios, consulte los manuales de usuario disponibles en las consolas de servicio.

Barra del historial de siete días

En la pantalla **Clientes**, la barra **historial de siete días** muestra el estado de las copias de seguridad de la carga de trabajo de cada inquilino de cliente durante los últimos siete días. La barra se divide en 168 líneas de colores. Cada línea representa un intervalo de una hora y muestra el peor estado de una copia de seguridad en el correspondiente intervalo.

La siguiente tabla proporciona información sobre el significado del color de las líneas.

Color	Descripción
rojo	al menos una de las copias de seguridad falló durante el periodo de una hora
naranja	al menos una de las copias de seguridad se completó con un aviso, pero sin errores, durante el periodo de una hora
verde	al menos una de las copias de seguridad se completó con éxito sin errores ni avisos durante el periodo de una hora
gris	no se completó ninguna copia de seguridad durante el periodo de una hora

La barra **historial de siete días** muestra "Sin copias de seguridad" hasta que se recopilan las estadísticas correspondientes.

Para inquilinos de socio, la barra **historial de siete días** está vacía ya que las estadísticas agregadas no son compatibles.

Las cuentas de usuario y los inquilinos

Hay dos tipos de cuentas de usuario: las cuentas de administrador y las cuentas de usuario.

- Los **Administradores** tienen acceso al portal de gestión. Tienen la función de administrador en todos los servicios.
- Los **Usuarios** no tienen acceso al portal de gestión. Su acceso a los servicios y sus funciones en los servicios están definidas por un administrador.

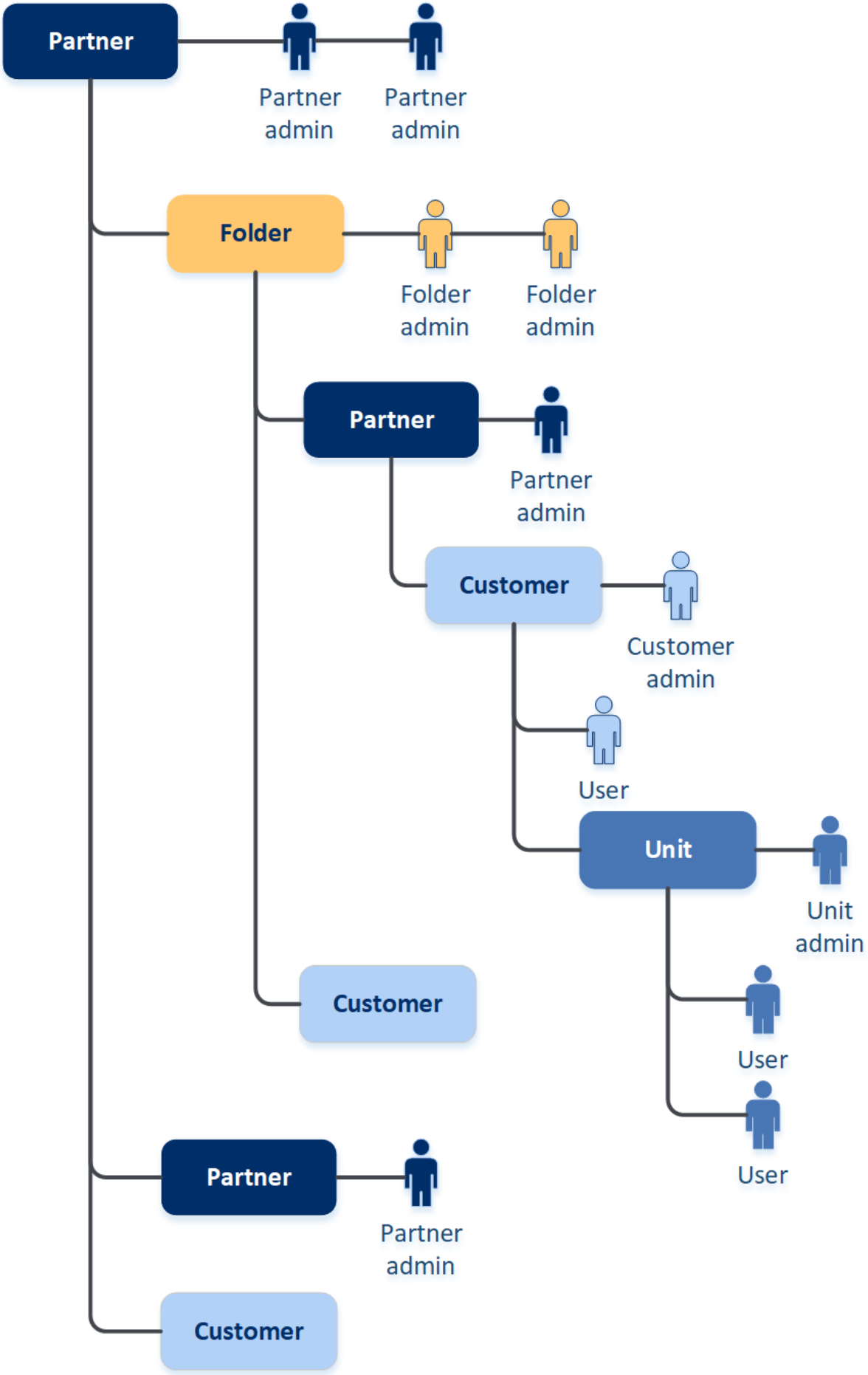
Cada cuenta pertenece a un inquilino. Un inquilino es una parte de los recursos del portal de gestión (como las cuentas de usuario y los inquilinos secundarios) y las ofertas de servicios (servicios habilitados y elementos ofertados en ellos) dedicadas a un socio o a un cliente. Se supone que la jerarquía del inquilino ajusta las relaciones cliente/proveedor entre los usuarios del servicio y los proveedores.

- Habitualmente, el tipo de inquilino **Socio** corresponde a proveedores de servicio que revenden los servicios.
- Un tipo de inquilino **Carpeta** es un inquilino suplementario que habitualmente usan los administradores de socios para agrupar socios y clientes con la finalidad de configurar ofertas independientes y/o distinta personalización de marca.
- Un tipo de inquilino **Cliente** suele corresponder a organizaciones que usan los servicios.
- Un tipo de inquilino **Unidad** suele corresponder a unidades o departamentos de la organización.

Un administrador puede crear y gestionar inquilinos, cuentas de administrador y cuentas de usuario en su mismo nivel jerárquico o en cualquier nivel inferior.

Un administrador del tipo de inquilino principal **Partner** puede actuar como administrador de un nivel inferior en inquilinos del tipo **Cliente** o **Partner**, cuyo modo de gestión es **Gestionado por el proveedor del servicio**. De este modo, el administrador de nivel partner puede, por ejemplo, gestionar cuentas de usuario y servicios, o acceder a copias de seguridad y otros recursos en el inquilino secundario. No obstante, los administradores del nivel más bajo pueden limitar el acceso de administradores de mayor nivel a su inquilino.

El diagrama que se muestra a continuación ilustra un ejemplo de jerarquía de los inquilinos socio, carpeta, cliente y unidad.


Partner
Partner admin
Partner admin
Folder
Folder admin
Folder admin
Partner
Partner admin
Customer
Customer admin
User
Unit
Unit admin
User
User
Customer
Partner
Partner admin
Customer

En la siguiente tabla se resumen las operaciones que pueden realizar los administradores y usuarios.

Operación	Usuarios	Administradores de clientes y unidades	Administradores de socios y carpetas
Crear inquilinos	No	Sí	Sí
Crear cuentas	No	Sí	Sí
Descargar e instalar el software.	Sí	Sí	No*
Gestionar servicios	Sí	Sí	Sí
Crear informes acerca del uso del servicio	No	Sí	Sí
Configurar personalización de marca	No	No	Sí

*Un administrador de socios que deba realizar estas operaciones puede crear un administrador de cliente o una cuenta de usuario para su propio uso.

Gestión de inquilinos

Los siguientes inquilinos están disponibles en Cyber Protect:

- Normalmente se crea un inquilino **Socio** para cada socio que firma el acuerdo de asociación.
- Normalmente se crea un inquilino **Carpeta** para agrupar socios y clientes con la finalidad de configurar ofertas independientes y/o distinta personalización de marca.
- Normalmente se crea un grupo **Cliente** para cada organización que contrata un servicio.
- Se crea un inquilino **Unidad** dentro de un inquilino cliente para expandir el servicio a una nueva unidad organizativa.

Los pasos para crear y configurar un inquilino varían en función del inquilino que cree, pero, en general, el proceso consta de estos pasos:

1. Crear el inquilino.
2. Seleccionar los servicios para el inquilino.
3. Configurar los elementos de oferta para el inquilino.

Creación de un inquilino

1. Inicie sesión en el portal de gestión.
2. Vaya hasta el inquilino en el que desee crear un inquilino.

3. En la esquina superior derecha, haga clic en **Nuevo** y, a continuación, haga clic en una de las siguientes opciones dependiendo del tipo de inquilino que desee crear:
   - Normalmente se crea un inquilino **Socio** para cada socio que firma el acuerdo de asociación.
   - Normalmente se crea un inquilino **Carpeta** para agrupar socios y clientes con la finalidad de configurar ofertas independientes y/o distinta personalización de marca.
   - Normalmente se crea un grupo **Cliente** para cada organización que contrata un servicio.
   - Se crea un inquilino **Unidad** dentro de un inquilino cliente para expandir el servicio a una nueva unidad organizativa.
4. En **Nombre**, especifique un nombre para el nuevo inquilino.
5. [Solo cuando cree un inquilino de partner] Ingrese **Nombre oficial (legal) de la empresa** (obligatorio) y el **número de IVA/código fiscal/número de registro de la empresa** (opcional).
6. [Solamente al crear un inquilino cliente] En **Modo**, seleccione si el inquilino usa los servicios en el modo de prueba o en el modo de producción. Los informes de uso del servicio mensuales no incluyen datos de uso para inquilinos que utilizan el modo de prueba.

   Importante
   Si cambia del modo de prueba al modo de producción a mitad de mes, se incluirá todo el mes en el informe de uso del servicio. Por este motivo, le recomendamos que cambie de modo el primer día del mes. El modo se cambia automáticamente a producción cuando un inquilino permanece en el modo de prueba durante todo un mes.
   Hay dos posibles escenarios para cambiar automáticamente el modo de prueba de los inquilinos a producción:
   - A mitad de mes, en cuyo caso se incluirá todo el mes ***siguiente*** en el informe de uso del servicio mensual.
   - [Opción recomendada] El primer día del mes. En ese caso, solo se tendrá en cuenta el mes en curso.

7. En el **Modo de gestión**, seleccione uno de los siguientes modos para gestionar el acceso al inquilino:
   - **Autoservicio**: este modo limita el acceso a este inquilino para administradores del inquilino principal: solo pueden modificar las propiedades del inquilino, pero no pueden acceder ni gestionar nada en su interior (por ejemplo, inquilinos, usuarios, servicios, copias de seguridad y otros recursos).
   - **Gestionado por el proveedor de servicio**: este modo otorga a los administradores del inquilino principal acceso completo al inquilino: modificar propiedades, gestionar inquilinos, usuarios y servicios; acceso a las copias de seguridad y otros recursos.

   Solo el administrador del inquilino que usted haya creado podrá cambiar el Modo de gestión si este es **Autoservicio**. Para ello, el administrador del inquilino creado puede ir a **Configuración** > **Seguridad** y establecer el conmutador **Acceso al soporte técnico**.
   Puede comprobar el modo de gestión seleccionado para sus inquilinos secundarios en la pestaña **Clientes**.

8. En **Seguridad**, habilite o deshabilite la autenticación de doble factor para el inquilino.
   Si está habilitada, todos los usuarios de este inquilino deberán establecer la autenticación de doble factor en sus cuentas para que el acceso sea más seguro. Los usuarios deben instalar la aplicación de autenticación en sus dispositivos de segundo factor y utilizar los códigos TOTP de un solo uso generados, además de las credenciales y contraseñas tradicionales, para iniciar sesión en la consola. Para obtener más información, consulte "Establecimiento de la autenticación de doble factor". Para ver el estado de la autenticación de doble factor de sus clientes, vaya a **Clientes**.
9. [Solo cuando se cree un inquilino de cliente en el modo de seguridad aumentada] En **Seguridad**, seleccione la casilla de verificación **Modo de seguridad aumentada**.
   Con este modo, solo se permiten copias de seguridad cifradas. La contraseña de cifrado debe establecerse en el dispositivo protegido. Sin ella, las copias de seguridad no se podrán realizar. Todas las operaciones que requieren proporcionar la contraseña de cifrado a un servicio en la nube no están disponibles en este modo. Para obtener más información, consulte "Modo Seguridad aumentada" (p. 38).

   Importante
   El modo Seguridad aumentada no se puede deshabilitar una vez que se ha creado el inquilino.

10. En **Crear administrador**, configure una cuenta de administrador.

    Nota
    La creación de un administrador es obligatoria para un inquilino cliente y un inquilino partner con el **Modo de gestión** establecido en **Autoservicio**.

    a. Introduzca un nombre de inicio de sesión y un correo electrónico para la cuenta de administrador. El resto de campos son opcionales, pero proporcionan más canales de comunicación por si es necesario contactar con el administrador.
    b. Seleccione un idioma.
       Se utilizará el inglés de manera predeterminada si no selecciona ninguno.
    c. Especifique las los contactos de empresa.
       - **Facturación**: el contacto que recibirá actualizaciones sobre cambios importantes en la creación de informes de uso en la plataforma.
       - **Técnico**: el contacto que recibirá actualizaciones sobre cambios técnicos importantes en la plataforma.
       - **Comercial**: el contacto que recibirá actualizaciones sobre cambios comerciales importantes en la plataforma.

         Puede asignar más de un contacto de la empresa a un usuario.
11. En **Idioma**, cambie el idioma predeterminado de las notificaciones, los informes y el software que se usarán para este inquilino.
12. Realice uno de los siguientes procedimientos:
    - Para finalizar la creación del inquilino, haga clic en **Guardar y cerrar**. En este caso, todos los servicios se habilitarán para el inquilino. Se establecerá el modo de facturación por carga de

trabajo para el servicio Protección.

- Para seleccionar los servicios para el inquilino, haga clic en **Siguiente**. Consulte "Pasos para gestionar los servicios para un inquilino" (p. 39).

Modo Seguridad aumentada

El modo Seguridad aumentada tiene una configuración especial para clientes con demandas de seguridad aumentadas. Este modo requiere cifrado obligatorio para todas las copias de seguridad y permite establecer contraseñas de cifrado solo de manera local.

Un administrador de socios solo podrá habilitar el modo Seguridad aumentada cuando cree un nuevo inquilino de cliente y no lo podrá deshabilitar más tarde. No se puede habilitar el modo Seguridad aumentada para clientes que ya existan.

Con el modo Seguridad aumentada, todas las copias de seguridad creadas en un inquilino de cliente y sus unidades se cifrarán automáticamente con el algoritmo AES y una clave de 256 bits. Los usuarios solo podrán establecer sus contraseñas de cifrado en los dispositivos protegidos y no podrán configurar las claves de cifrado en los planes de protección.

Los servicios en la nube no pueden acceder a las contraseñas de cifrado. Debido a esta restricción, las siguientes características no están disponibles para los inquilinos en el modo Seguridad aumentada:

- Recuperación mediante la consola de servicio
- Examen de copias de seguridad a nivel de archivo mediante la consola de servicio
- Copia de seguridad de la nube a la nube
- Copia de seguridad de sitios web
- Copia de seguridad de aplicación
- Copia de seguridad de dispositivos móviles
- Análisis antimalware de copias de seguridad
- Recuperación segura
- Creación automática de listas blancas corporativas
- Mapa de protección de datos
- Recuperación ante desastres
- Informes y paneles de control relacionados con las características no disponibles

Limitaciones

- El modo Seguridad aumentada solo es compatible con los agentes con la versión 15.0.26390 o posterior.
- El modo Seguridad aumentada no está disponible para dispositivos que ejecuten Red Hat Enterprise Linux 4.x o 5.x y sus derivados.

Pasos para gestionar los servicios para un inquilino

Cuando cree un nuevo inquilino, se activarán todos los servicios de forma predeterminada. Puede seleccionar qué servicios estarán disponibles para los usuarios del inquilino y sus inquilinos secundarios.

También puede seleccionar y habilitar servicios para varios inquilinos existentes con una acción. Para obtener más información, consulte "Habilitación de servicios para varios inquilinos existentes" (p. 40).

Este procedimiento no se aplica a un inquilino unidad.

Pasos para seleccionar los servicios para un inquilino

1. En la sección **Seleccionar servicios** del cuadro de diálogo crear/editar inquilino, seleccione un modo de facturación o una edición.
   - Seleccione el modo de facturación **Por carga de trabajo** o **Por gigabyte** y, a continuación, deseleccione las casillas de verificación de los servicios que desea desactivar para el inquilino. El conjunto de servicios de ambos modos de facturación es idéntico.

     Para la recuperación ante desastres avanzada, si ha registrado su propia ubicación para la recuperación ante desastres en su cuenta, puede seleccionar la ubicación de la lista desplegable.
   - Para utilizar la edición heredada, seleccione el botón de opción **Ediciones heredadas** y seleccione una edición de la lista desplegable.

   Los servicios deshabilitados no serán visibles para los usuarios del inquilino y sus inquilinos secundarios.
2. Realice uno de los siguientes procedimientos:
   - Para finalizar la creación del inquilino, haga clic en **Guardar y cerrar**. En este caso, todos los elementos de oferta para los servicios seleccionados se activarán para el inquilino con una cuota ilimitada.
   - Para configurar los elementos de oferta para el inquilino, haga clic en **Siguiente**. Consulte "Configuración de los elementos de oferta para un inquilino" (p. 39).

Configuración de los elementos de oferta para un inquilino

Cuando cree un nuevo inquilino, se activarán todos los elementos de oferta para los servicios seleccionados. Puede seleccionar qué artículos de oferta desactivados estarán disponibles para los usuarios del inquilino y sus inquilinos secundarios y establecer cuotas.

Este procedimiento no se aplica a un inquilino unidad.

Pasos para configurar los elementos de oferta para un inquilino

1. En la sección **Configurar servicios** del cuadro de diálogo crear/editar inquilino, debajo de cada pestaña de servicio, deseleccione las casillas de verificación de los elementos ofrecidos que desea desactivar.

La funcionalidad correspondiente a los artículos de oferta deshabilitados no estará disponible para los usuarios del inquilino y sus inquilinos secundarios.

Nota
Puede desactivar los elementos de oferta relacionados con la funcionalidad de protección avanzada, pero se reactivarán automáticamente cuando un usuario active una característica avanzada de un plan de protección.

2. Algunos servicios permiten seleccionar los almacenamientos que estarán disponibles para el inquilino nuevo. Los almacenamientos se agrupan por ubicaciones. Puede realizar selecciones en la lista de ubicaciones y almacenamientos disponibles para su inquilino.
   - Al crear un inquilino socio/carpeta, puede seleccionar diversos almacenamientos y ubicaciones para cada servicio.
   - Al crear un inquilino cliente, tiene que seleccionar una ubicación y, luego, un almacenamiento por servicio dentro de esta ubicación. Los almacenamientos asignados al cliente se pueden cambiar más adelante, pero únicamente si su uso es 0 GB, es decir, antes de que el cliente empiece a usarlos o después de que el cliente elimine todas las copias de seguridad de ese almacenamiento. La información sobre el uso del espacio de almacenamiento no se actualiza en tiempo real. Por favor, espere 24 horas para que la información se actualice.

   Para obtener más información sobre los almacenamientos, consulte "Gestión de ubicaciones y almacenamiento".
3. Para especificar la cuota de un artículo, haga clic en el enlace **Ilimitada** junto al artículo de oferta.
   Estas cuotas son de advertencia. Si se sobrepasa cualquiera de estos valores, se envía una notificación por correo electrónico a los administradores del inquilino y a los administradores del inquilino principal. No se aplican restricciones al uso de los servicios. En el caso de un inquilino partner, se espera que el uso del artículo ofertado pueda superar la cuota porque no se puede establecer un límite de exceso cuando se crea este tipo de inquilino.
4. [Solamente al crear un inquilino cliente] Especifique los usos por encima del límite de la cuota. Un uso por encima del límite permite a un inquilino cliente sobrepasar la cuota en un valor especificado. Si el uso por encima del límite se sobrepasa, se aplican las restricciones sobre el uso del servicio correspondiente.
5. Haga clic en **Guardar y cerrar**.

El inquilino creado recientemente aparece en la pestaña **Clientes** de la consola de gestión.

Si desea modificar la configuración del inquilino o cambiar de administrador, seleccione el inquilino en la pestaña **Clientes** y luego haga clic en el icono de lápiz en la sección que desea modificar.

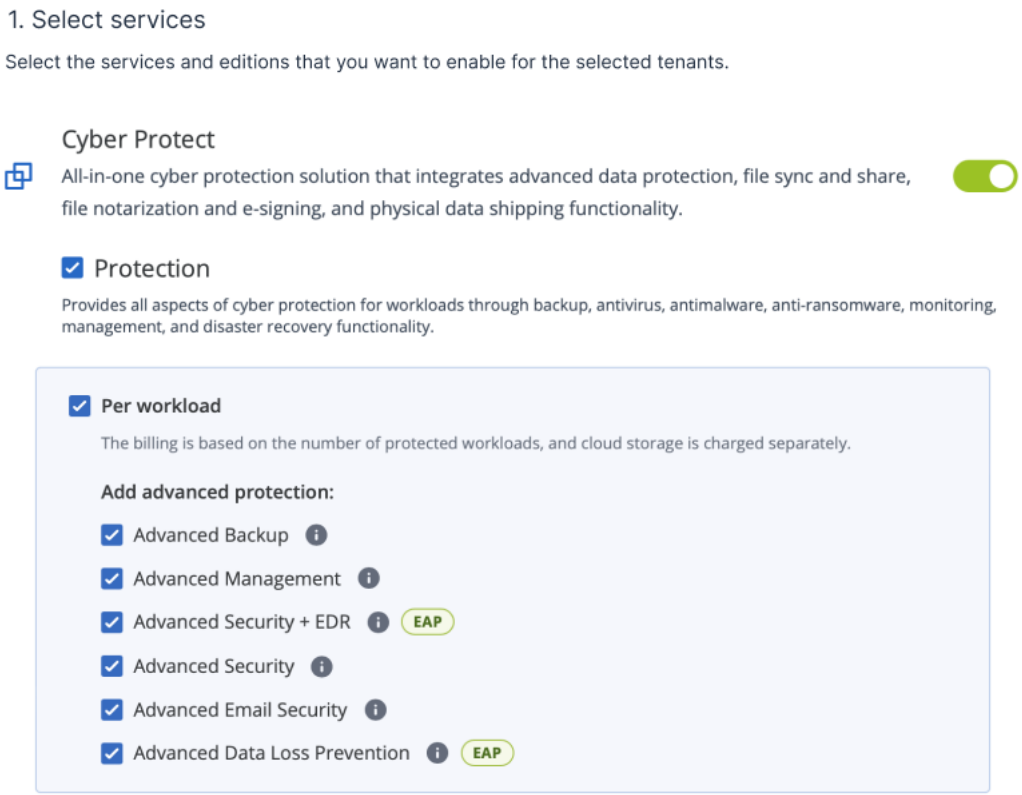
Habilitación de servicios para varios inquilinos existentes

Puede habilitar varios servicios, ediciones, paquetes y artículos de oferta para varios inquilinos (hasta un máximo de 100 inquilinos en una sesión).

Este procedimiento se aplica a inquilinos de subraíz, partner, carpeta y cliente. Los inquilinos de cualquiera de estos tipos se pueden seleccionar simultáneamente.

Pasos para habilitar servicios para varios inquilinos

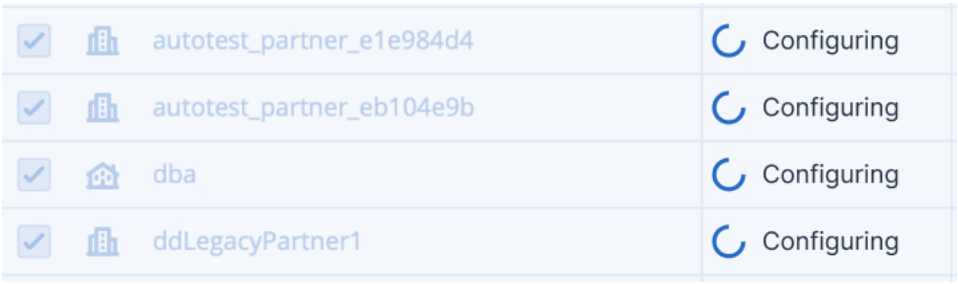
1. En el portal de gestión, vaya a **Clientes**.
2. En la esquina superior derecha, haga clic en **Configurar servicios**.
3. Seleccione los inquilinos para los que desea habilitar servicios mediante la selección de la casilla de verificación junto al nombre del inquilino y luego haga clic en **Siguiente**.
4. En la sección **Seleccionar servicios**, seleccione los servicios correspondientes que desee aplicar a todos los inquilinos seleccionados y haga clic en **Siguiente**.



Nota
No puede deshabilitar un servicio habilitado previamente en esta pantalla. Todos los servicios, ediciones y artículos de oferta seleccionados antes de comenzar este procedimiento seguirán habilitados.

5. En la sección **Configurar servicios**, seleccione las funciones del servicio y los artículos de oferta que desee habilitar para los inquilinos seleccionados y haga clic en **Siguiente**.
6. En la sección **Resumen**, revise los cambios que se aplicarán a los inquilinos seleccionados.
   Puede hacer clic en **Expandir todos** para ver todos los artículos de oferta y los servicios seleccionados de inquilino que se aplicarán. De manera alternativa, puede expandir cada inquilino para ver los servicios seleccionados y artículos de oferta específicos de ese inquilino.

7. Haga clic en **Aplicar cambios**. Si bien los servicios se configuran para cada inquilino, el inquilino está deshabilitado y la columna **Estado del inquilino** indica los servicios y artículos de oferta que se están configurando, como se muestra a continuación.



8. Cuando la configuración de servicios y artículos de oferta se aplique correctamente a los inquilinos seleccionados, se mostrará un mensaje de confirmación.
   Si por algún motivo los servicios y artículos de oferta no pudiesen aplicarse a un inquilino, la columna **Estado del inquilino** muestra **No aplicado**. Haga clic en **Inténtelo de nuevo** para revisar la configuración de los inquilinos seleccionados.

Activación de las notificaciones de mantenimiento

Como usuario del partner, puede permitir que sus inquilinos secundarios (partners y clientes) reciban correos electrónicos de notificación de mantenimiento directamente desde el centro de datos de Cyber Protect, así como notificaciones de mantenimiento incorporadas dentro del portal de administración. Esto le ayudará a reducir el número de llamadas al soporte técnico relacionadas con el mantenimiento.

Nota
Los correos electrónicos de notificación de mantenimiento llevan la marca del centro de datos. La adaptación de marca personalizada no se admite en estas notificaciones.

Pasos para activar las notificaciones de mantenimiento de los partners o clientes secundarios

1. Inicie sesión en el portal de administración como usuario del partner, haga clic en **Clientes** y, a continuación, haga clic en el nombre de un inquilino del partner o cliente para el que desee activar las notificaciones de mantenimiento.
2. Haga clic en **Configurar**.
3. En la pestaña **Configuración general**, localice la opción **Notificaciones de mantenimiento** y actívela.
   Si no ve la opción **Notificaciones de mantenimiento**, póngase en contacto con su proveedor de servicios.

Nota
Las notificaciones de mantenimiento se han activado, pero no se enviarán hasta que el inquilino seleccionado active las notificaciones para sus usuarios o propague esta opción a los partners o clientes secundarios para que activen las notificaciones para sus usuarios.

Pasos para activar las notificaciones de mantenimiento de un usuario

1. Inicie sesión en el portal de administración como usuario del partner o como administrador de la empresa.
   Como partner, puede acceder a los usuarios de todos los inquilinos que gestiona.
2. Vaya a **Gestión empresarial** > **Usuarios** y, a continuación, haga clic en el nombre de un usuario para el que desee activar las notificaciones de mantenimiento.
3. En la pestaña **Servicios**, en la sección **Configuración**, pulse el lápiz para editar las opciones.
4. Seleccione la casilla de verificación **Notificaciones de mantenimiento** y haga clic en **Listo**.

El usuario seleccionado recibirá notificaciones por correo electrónico sobre las próximas actividades de mantenimiento en el centro de datos.

Configuración del perfil del cliente administrado de forma automática

Como partner, puede configurar los perfiles de los clientes administrados de forma automática de los inquilinos que gestione. Esta opción le permite controlar la visibilidad del perfil de los inquilinos y la información de contacto de cada uno de sus clientes.

Pasos para configurar el perfil del cliente administrado de forma automática

1. En el portal de gestión, vaya a **Clientes**.
2. Seleccione el cliente para el que desea configurar el perfil administrado de forma automática.
3. Seleccione la pestaña **Configuración** y, a continuación, seleccione la pestaña **Configuración general**.
4. Active o desactive el conmutador **Habilitar perfil del cliente administrado de forma automática**.

Cuando se habilite el perfil del cliente administrado de forma automática, este cliente verá la sección **Perfil de empresa** en el menú de navegación y los campos relacionados con el contacto en el asistente de creación de usuarios (**teléfono del trabajo**, **contacto de la empresa** y **puesto**).

Cuando se deshabilite el perfil del cliente administrado de forma automática, se ocultará la sección **Perfil de empresa** en el menú de navegación y los campos relacionados con el contacto en el asistente de creación de usuarios.

Configuración de los contactos de la empresa

Como partner, puede configurar la información de contacto de su empresa y la de los inquilinos que gestione. Enviaremos actualizaciones sobre las nuevas características y otros cambios importantes de la plataforma a los contactos de esta lista.

Puede añadir varios contactos y asignar contactos de empresa en función del rol del usuario. Puede crear contactos de usuarios que existan en la plataforma de Cyber Protect o añadir la información de contacto de las personas que no tengan acceso al servicio.

Pasos para configurar los contactos de su empresa

1. En la consola de administración, vaya a **Gestión empresarial** > **Perfil de empresa**.
2. En la sección **Contactos**, haga clic en **+**.
3. Seleccione una opción para crear el contacto.
   - **Crear a partir de usuario existente**
     - Seleccione un usuario de la lista desplegable.
     - Seleccione un contacto de la empresa.
       - **Facturación**: el contacto que recibirá actualizaciones sobre cambios importantes en la creación de informes de uso en la plataforma.
       - **Técnico**: el contacto que recibirá actualizaciones sobre cambios técnicos importantes en la plataforma.
       - **Comercial**: el contacto que recibirá actualizaciones sobre cambios comerciales importantes en la plataforma.

         Puede asignar más de un contacto de la empresa a un usuario.

       Si elimina un contacto asociado a un usuario de la lista de contactos del perfil Empresa, el usuario no se eliminará. El sistema anulará la asignación de todos los conctacto de la empresa para el usuario, por lo que ya no aparecerá en la columna **Contactos de la empresa** de la lista **Usuarios**.

       Si desea cambiar la dirección de correo electrónico del contacto que está asociado con el usuario, el sistema solicitará la verificación de la nueva dirección que defina. Se enviará un correo electrónico a esta dirección y el usuario deberá confirmar el cambio.
   - **Crear un contacto nuevo**
     - Proporcione la información del contacto.
       - **Nombre**: nombre de la persona de contacto. Este campo es obligatorio.
       - **Apellidos**: apellidos de la persona de contacto. Este campo es obligatorio.
       - **Dirección de correo electrónico de empresa**: dirección de correo electrónico de la persona de contacto. Este campo es obligatorio.
       - **Teléfono del trabajo**: este campo es opcional.
       - **Puesto**: este campo es opcional.
     - Seleccione los **Contactos de la empresa**.
       - **Facturación**: el contacto que recibirá actualizaciones sobre cambios importantes en la creación de informes de uso en la plataforma.
       - **Técnico**: el contacto que recibirá actualizaciones sobre cambios técnicos importantes en la plataforma.
       - **Comercial**: el contacto que recibirá actualizaciones sobre cambios comerciales importantes en la plataforma.

         Puede asignar más de un contacto de la empresa a un usuario.
4. Haga clic en **Agregar**.

Pasos para configurar contactos para un inquilino

Nota
Si modifica la información de contacto para un inquilino secundario, los cambios serán visibles para el inquilino.

1. En el portal de gestión, vaya a **Clientes**.
2. Haga clic en el inquilino y en **Configurar**.
3. En la sección **Contactos**, haga clic en **+**.
4. Seleccione una opción para crear el contacto.
   - **Crear a partir de usuario existente**
     - Seleccione un usuario de la lista desplegable.
     - Seleccione un contacto de la empresa.
       - **Facturación**: el contacto que recibirá actualizaciones sobre cambios importantes en la creación de informes de uso en la plataforma.
       - **Técnico**: el contacto que recibirá actualizaciones sobre cambios técnicos importantes en la plataforma.
       - **Comercial**: el contacto que recibirá actualizaciones sobre cambios comerciales importantes en la plataforma.

         Puede asignar más de un contacto de la empresa a un usuario.

       Si elimina un contacto asociado a un usuario de la lista de contactos del perfil Empresa, el usuario no se eliminará. El sistema anulará la asignación de todos los conctacto de la empresa para el usuario, por lo que ya no aparecerá en la columna **Contactos de la empresa** de la lista **Usuarios**.

       Si desea cambiar la dirección de correo electrónico del contacto que está asociado con el usuario, el sistema solicitará la verificación de la nueva dirección que defina. Se enviará un correo electrónico a esta dirección y el usuario deberá confirmar el cambio.
   - **Crear un contacto nuevo**
     - Proporcione la información del contacto.
       - **Nombre**: nombre de la persona de contacto. Este campo es obligatorio.
       - **Apellidos**: apellidos de la persona de contacto. Este campo es obligatorio.
       - **Dirección de correo electrónico de empresa**: dirección de correo electrónico de la persona de contacto. Este campo es obligatorio.
       - **Teléfono del trabajo**: este campo es opcional.
       - **Puesto**: este campo es opcional.
     - Seleccione los **Contactos de la empresa**.
       - **Facturación**: el contacto que recibirá actualizaciones sobre cambios importantes en la creación de informes de uso en la plataforma.
       - **Técnico**: el contacto que recibirá actualizaciones sobre cambios técnicos importantes en la plataforma.

- **Comercial**: el contacto que recibirá actualizaciones sobre cambios comerciales importantes en la plataforma.

  Puede asignar más de un contacto de la empresa a un usuario.

5. Haga clic en **Agregar**.

Actualizar los datos de uso para un inquilino

De forma predeterminada, los datos de uso se actualizan en intervalos fijos. Puede actualizar manualmente los datos de uso para un inquilino.

1. En la consola de gestión, vaya a **Clientes**.
2. Haga clic en el inquilino y en los puntos suspensivos que se encuentran en la fila de inquilino.
3. Seleccione **Actualizar uso**.

   Nota
   Puede llevar hasta 10 minutos recuperar los datos.

4. Recargue la página para ver los datos actualizados.

Deshabilitación y habilitación de un inquilino

Es posible que tenga que deshabilitar temporalmente a un inquilino. Por ejemplo, en caso de que su inquilino tenga deudas por usar los servicios.

Cómo deshabilitar un inquilino

1. En el portal de gestión, vaya a **Clientes**.
2. Seleccione el inquilino que desee deshabilitar y, a continuación, haga clic en el icono de elipsis > **Deshabilitar**.
3. Haga clic en **Deshabilitar** para confirmar la acción.

Como resultado:

- Se deshabilitarán el inquilino y todos sus subinquilinos, y se interrumpirán sus servicios.
- La facturación del inquilino y de sus subinquilinos seguirá adelante, ya que sus datos se conservarán y almacenarán en Cyber Protect Cloud.
- Se deshabilitarán todos los clientes API del inquilino y sus subinquilinos, y todas las integraciones que usen estos clientes dejarán de funcionar.

Para habilitar un inquilino, selecciónelo de la lista de clientes y, a continuación, haga clic en el icono de elipsis > **Habilitar**.

Mover un inquilino a otro inquilino

El portal de gestión le permite mover un inquilino desde un inquilino principal a otro inquilino principal. Esto puede ser útil si desea transferir un cliente de un socio a otro, o si ha creado un

inquilino carpeta para organizar sus clientes y desea mover algunos de ellos al inquilino carpeta de reciente creación.

Tipo de inquilinos que se pueden mover

Tipo de inquilino	Se puede mover	Inquilino de destino
Socio	Sí	Partner o carpeta
Carpeta	Sí	Partner o carpeta
Cliente	Sí	Partner o carpeta
Unidad	No	Ninguno

Requisitos y restricciones

- Puede mover un inquilino solo si el inquilino principal de destino tiene el mismo o mayor conjunto de servicios y oferta que el inquilino principal original.
- Cuando se mueve un inquilino cliente, todos los almacenamientos asignados al inquilino cliente en el inquilino principal original deben existir en el inquilino principal de destino. Esto es obligatorio porque los datos del cliente relacionados con el servicio no se pueden mover de un almacenamiento a otro.
- En los inquilinos de cliente gestionados por proveedores de servicios, puede haber planes que se apliquen a las cargas de trabajo del cliente desde el nivel del proveedor de servicios (por ejemplo, planes de programación).

  Al mover dicho inquilino de cliente, los planes del proveedor de servicios se revocarán en las cargas de trabajo del cliente y todos los servicios asociados con estos planes dejarán de funcionar para este cliente.
- Puede mover inquilinos dentro de la jerarquía de cuentas del partner. También puede mover algunos inquilinos de cliente a un inquilino de destino fuera de la jerarquía de cuentas del partner. Para saber si la operación es posible, póngase en contacto con su gerente de cuenta en .
- Solo los administradores (por ejemplo, del portal de administración o de empresa) pueden mover inquilinos a diferentes inquilinos principales.

Cómo mover a un inquilino

1. Inicie sesión en el portal de gestión.
2. Busque y copie el **ID interno** del inquilino de la carpeta o partner de destino al que desea mover un inquilino. Realice lo siguiente:
   a. En la pestaña **Clientes**, seleccione el inquilino de destino al que desea mover un inquilino.
   b. En el panel de propiedades de inquilino, haga clic en el icono de elipsis vertical y, a continuación, en **Mostrar ID**.
   c. Copie la cadena de texto que aparece en el campo **ID interno** y haga clic en **Cancelar**.

3. Seleccione el inquilino que desea mover y, luego, muévalo a la carpeta o partner de destino. Realice lo siguiente:
   a. En la pestaña **Clientes**, seleccione el inquilino que desea mover.
   b. En el panel de propiedades de inquilino, haga clic en el icono de elipsis vertical, y luego haga clic en **Mover**.
   c. Pegue el identificador interno del inquilino de destino y luego haga clic en **Mover**.

La operación empieza inmediatamente y tarda hasta 10 minutos.

Si el inquilino que está moviendo tiene inquilinos secundarios (por ejemplo, es un inquilino de carpeta o partner con un inquilino de cliente dentro), todo el subárbol del inquilino se moverá al inquilino de destino.

Conversión de un inquilino socio en un inquilino carpeta y viceversa

Con el portal de gestión podrá convertir a un inquilino socio en un inquilino carpeta y viceversa.

Esto puede ser útil si ha usado un inquilino socio con fines de agrupación y ahora quiere organizar su infraestructura de inquilinos adecuadamente. Esto también es útil si quiere que en el panel de operaciones se incluya información adicional sobre el inquilino.

También puede convertir un inquilino carpeta en uno socio.

Nota
Esta conversión es una operación segura y no afecta a los usuarios del inquilino ni a ningún otro dato relacionado con el servicio.

Pasos para convertir a un inquilino

1. Inicie sesión en el portal de gestión.
2. En la pestaña **Clientes**, seleccione el inquilino que desea convertir.
3. Realice uno de los siguientes procedimientos:
   - Haga clic en el icono de puntos suspensivos situado junto al nombre del inquilino.
   - Seleccione el inquilino y, a continuación, haga clic en el icono de puntos suspensivos del panel de propiedades del inquilino.
4. Haga clic en **Convertir en carpeta** o en **Convertir en socio**.
5. Confirme su decisión.

Limitación del acceso a su inquilino

Los administradores del nivel del cliente y otros superiores pueden limitar el acceso a sus inquilinos para los administradores de nivel superior.

Si el acceso del inquilino está limitado, los administradores del inquilino principal solo pueden modificar las propiedades del inquilino. No pueden ver ni las cuentas ni los inquilinos secundarios en ningún caso.

Para impedir que los administradores de nivel superior puedan acceder a su inquilino

1. Inicie sesión en el portal de gestión.
2. Vaya a **Configuración** > **Seguridad**.
3. Deshabilite el conmutador **Acceso al soporte técnico**.

Como resultado, los administradores de los inquilinos principales tendrán acceso limitado a su inquilino. Solo podrán modificar las propiedades del inquilino, pero no acceder ni gestionar nada en su interior (por ejemplo, inquilinos, usuarios, servicios, copias de seguridad y otros recursos).

Si el conmutador **Acceso al soporte técnico** está habilitado, los administradores de los inquilinos principales tendrán acceso completo a su inquilino. Podrán hacer lo siguiente: modificar propiedades; gestionar inquilinos, usuarios y servicios; acceder a copias de seguridad y otros recursos.

Eliminación de un inquilino

Es posible que quiera eliminar un inquilino para liberar los recursos que usa. Las estadísticas de uso se actualizarán en el plazo de un día después de la eliminación. En aquellos inquilinos cuyo tamaño sea mayor, es posible que tarde más.

Antes de eliminar un inquilino, tiene que deshabilitarlo. Para obtener más información sobre cómo hacerlo, consulte: Deshabilitación y habilitación de un inquilino.

Importante
La eliminación de un inquilino es una acción irreversible.

Pasos para eliminar un inquilino

1. En el portal de gestión, vaya a **Clientes**.
2. Seleccione el inquilino que desee deshabilitar y, a continuación, haga clic en el icono > **Eliminar**.
3. Para confirmar su acción, introduzca su información de inicio de sesión y luego haga clic en **Eliminar**.

Como resultado:

- Se eliminarán el inquilino y sus subinquilinos.
- Se detendrán todos los servicios que se habilitaron en el inquilino y sus subinquilinos.
- Se eliminarán todos los usuarios del inquilino y sus subinquilinos.
- Todos los equipos que haya registrados en el inquilino y los subinquilinos dejarán de estarlo.
- Se eliminarán todos los datos relacionados con los servicios, por ejemplo, copias de seguridad y archivos sincronizados, del inquilino y los subinquilinos.
- Se eliminarán todos los clientes API del inquilino y sus subinquilinos, y todas las integraciones que usen estos clientes dejarán de funcionar.

Gestión de usuarios

Los administradores de partners, de clientes y de unidad pueden configurar y gestionar las cuentas de usuario de los inquilinos a los que pueden acceder.

Creación de una cuenta de usuario

Es posible que desee crear cuentas adicionales en los siguientes casos:

- Cuentas de administrador de socio/carpeta: para compartir las funciones de gestión de servicios con otras personas.
- Cuentas de administrador de cliente, unidad o cliente potencial: para delegar la gestión de los servicios en otras personas cuyos permisos de acceso estarán estrictamente limitados a la unidad, el cliente o el cliente potencial correspondiente.
- Cuentas de usuario en el cliente o un inquilino de unidad: para permitir que los usuarios solo puedan acceder a un subconjunto de servicios.

Tenga en cuenta que las cuentas existentes no se pueden mover entre inquilinos. Primero, necesita crear un inquilino y luego introducir cuentas.

Para crear una cuenta de usuario

1. Inicie sesión en el portal de gestión.
2. Vaya hasta el inquilino en el que desee crear una cuenta de usuario. Consulte "Navegación en el portal de gestión" (p. 29).
3. En la esquina superior derecha, haga clic en **Nuevo** > **Usuario**.
   De manera alternativa, vaya a **Gestión empresarial > Usuarios** y haga clic en **+ Nuevo**.
4. Especifique la siguiente información de contacto para la cuenta:
   - **Usuario**

     Importante
     Debe haber únicamente un usuario en cada cuenta.

   - **Correo electrónico**

     Importante
     Si el usuario está registrado en el servicio de File Sync & Share, facilite el correo electrónico que se utilizó para el registro de File Sync & Share.
     Tenga en cuenta que cada cuenta de usuario de cliente debe tener una dirección de correo electrónico única.

   - **Nombre**
   - **Apellidos**
   - [Opcional] **Teléfono del trabajo**

Nota
En el asistente de creación de usuarios solo se muestran campos como **Teléfono del trabajo**, **Puesto** y **Contacto de empresa** si el partner principal tiene habilitada la función **Habilitar perfil de usuario autogestionado** para el inquilino de cliente. De lo contrario, estos campos no aparecen.

- [Opcional] **Puesto**
- En **Idioma**, cambie el idioma predeterminado de las notificaciones, los informes y el software de esta cuenta.

5. [Opcional] Especifique los contactos de la empresa.
   - **Facturación**: el contacto que recibirá actualizaciones sobre cambios importantes en la creación de informes de uso en la plataforma.
   - **Técnico**: el contacto que recibirá actualizaciones sobre cambios técnicos importantes en la plataforma.
   - **Comercial**: el contacto que recibirá actualizaciones sobre cambios comerciales importantes en la plataforma.

     Puede asignar más de un contacto de la empresa a un usuario.

   Puede ver los contactos de empresa asignados para un usuario en la lista **Usuarios**, en la columna **Contactos de la empresa**, y editar la cuenta de usuario para cambiar los contactos de empresa si es necesario.
6. [No disponible cuando se crea una cuenta en un inquilino socio/carpeta] Seleccione los servicios a los que tendrá acceso el usuario y las funciones en cada servicio.

   Los servicios disponibles dependen de los servicios habilitados para el inquilino en el que se ha creado la cuenta de usuario.
   - Si selecciona la opción **Administrador de la compañía**, el usuario tendrá acceso al portal de gestión y a la función de administrador en todos los servicios actualmente habilitados para el inquilino. El usuario también tendrá la función de administrador en todos los servicios que se habiliten para el inquilino en el futuro.
   - Si selecciona la opción **Administrador de unidad**, el usuario tendrá acceso al portal de gestión, pero que tenga la función de administrador del servicio dependerá del servicio.
   - De lo contrario, el usuario tendrá las funciones seleccionadas en los servicios que seleccione.
7. Haga clic en **Crear**.

La cuenta de usuario creada recientemente aparece en la pestaña **Usuarios** de **Gestión empresarial**.

Si desea modificar la configuración del usuario o especificar parámetros de notificación o cuotas para el usuario (no disponible para administradores de partners y carpetas), seleccione al usuario en la pestaña **Usuarios** y haga clic en el icono de lápiz de la sección que desea modificar.

Pasos para restablecer la contraseña de un usuario

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. Seleccione el usuario cuya contraseña desee restablecer y, a continuación, haga clic en el icono > **Restablecer contraseña**.
3. Haga clic en **Restablecer** para confirmar la acción.

En este momento el usuario puede completar el proceso de restablecimiento si sigue las instrucciones incluidas en el correo electrónico que ha recibido.

En el caso de los servicios que no son compatibles con la autenticación de doble factor (por ejemplo, el registro en Cyber Infrastructure) es posible que deba convertir una cuenta de usuario en una *Cuenta de servicio*, la cual no requiere la autenticación de doble factor.

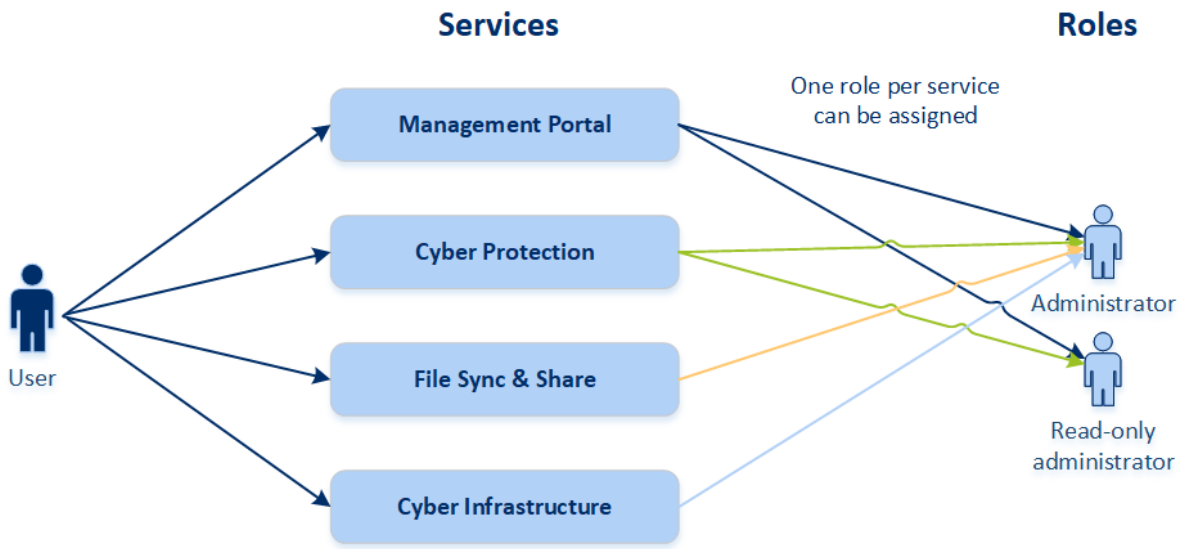
Pasos para convertir una cuenta de usuario al tipo de cuenta de servicio

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. Seleccione el usuario cuya cuenta desee convertir al tipo de cuenta de servicio y, a continuación, haga clic en el icono de los tres puntos > **Marcar como cuenta de servicio**.
3. En la ventana de confirmación, introduzca el código de autenticación de doble factor y confirme su acción.

Ahora la cuenta puede utilizarse para servicios que no son compatibles con la autenticación de doble factor.

Funciones de usuario disponibles para cada servicio

Un usuario puede tener varias funciones, pero solo una por servicio.



Para cada servicio, puede definir qué función se asignará a un usuario.

Servicio	Rol	Descripción

n/d	Administrador de la compañía	Este rol concede todos los derechos de administrador de todos los servicios. Este rol concede acceso a la lista blanca corporativa. Si el complemento Recuperación ante desastres del servicio Cyber Protection está activado para la empresa, este rol también permite acceder a la funcionalidad de recuperación ante desastres.
Portal de gestión	Administrador	Este rol concede acceso al portal de gestión, donde el administrador puede gestionar a los usuarios dentro de toda la organización.
	Administrador de solo lectura Nivel de partner	Esta función proporciona acceso de solo lectura a todos los objetos del portal de administración del partner y a los portales de administración de todos los clientes de este partner. Estos usuarios pueden acceder a los datos de otros usuarios de la organización en modo de solo lectura.
	Administrador de solo lectura Nivel de cliente	Esta función proporciona acceso de solo lectura a todos los objetos del portal de administración de toda la empresa. Estos usuarios pueden acceder a los datos de otros usuarios de la organización en modo de solo lectura.
	Administrador de solo lectura Nivel de unidad	Esta función proporciona acceso de solo lectura a todos los objetos del portal de administración de la unidad y subunidades de la empresa. Estos usuarios pueden acceder a los datos de otros usuarios de la organización en modo de solo lectura.
Cyber Protection	Administrador de cibernética	Además de los derechos del rol de administrador, este rol permite configurar y gestionar el servicio de Cyber Protection, así como aprobar acciones en Programación cibernética. El rol de administrador de cibernética solo está disponible para los inquilinos con el paquete de Advanced Management habilitado.
	Administrador	Este rol permite configurar y gestionar Cyber Protection para sus clientes. Este rol es necesario para configurar y gestionar la funcionalidad de Recuperación ante desastres y la lista de permitidos corporativa.
	Administrador de solo lectura	La función proporciona acceso de solo lectura a todos los objetos del servicio Cyber Protection. Estos usuarios pueden acceder a los datos de otros usuarios de la organización en modo de solo lectura. El administrador de solo lectura no puede configurar ni gestionar la funcionalidad de Recuperación ante desastres ni la lista blanca corporativa.
	Restaurar operador	El rol proporciona acceso a las copias de seguridad de las organizaciones de Microsoft 365 y Google Workspace y permite su recuperación, al mismo tiempo que restringe el acceso a contenido confidencial.

File Sync & Share	Administrador	Esta función permite configurar y gestionar File Sync & Share para sus usuarios.
Cyber Infrastructure	Administrador	Esta función permite configurar y gestionar Cyber Infrastructure para sus usuarios.

Función de administrador de solo lectura

Una cuenta con este rol tiene acceso de solo lectura a la consola web de Cyber Protection y puede hacer lo siguiente:

- Recopilar datos de diagnóstico, como informes del sistema.
- Ver todos los puntos de recuperación de una copia de seguridad, pero no profundizar en los contenidos de esta ni ver archivos, carpetas ni correos electrónicos.

Un administrador de solo lectura no puede hacer lo siguiente:

- Iniciar o detener ninguna tarea.
  Por ejemplo, un administrador de solo lectura no puede iniciar una recuperación o detener una copia de seguridad que esté en curso.
- Acceder al sistema de archivos en equipos de origen o de destino.
  Por ejemplo, un administrador de solo lectura no puede ver archivos, carpetas ni correos electrónicos en un equipo del que se ha realizado una copia de seguridad.
- Cambiar ninguna configuración.
  Por ejemplo, un administrador de solo lectura no puede crear un plan de protección ni cambiar ninguna de sus configuraciones.
- Crear, actualizar o eliminar ningún tipo de datos.
  Por ejemplo, un administrador de solo lectura no puede borrar copias de seguridad.

Todos los objetos de la interfaz de usuario que no son accesibles para un administrador de solo lectura están ocultos, excepto en el caso de la configuración predeterminada del plan de protección. Esta configuración sí se muestra, pero el botón **Guardar** no está activo.

Todos los cambios relacionados con las cuentas y los roles se muestran en la pestaña **Actividades** con la siguiente información:

- Qué es lo que ha cambiado
- Quién realizó cada cambio
- La fecha y hora de los cambios

Rol de operador de restauración

Este rol solo está disponible en el servicio Cyber Protection y está limitado a copias de seguridad de Microsoft 365 y Google Workspace.

Un operador de restauración puede:

- Ver alertas y actividades.
- Examinar y actualizar la lista de copias de seguridad.
- Examinar copias de seguridad sin acceder al contenido. El operador de restauración puede ver los nombres de los archivos de la copia de seguridad y el asunto y los emisores de los correos electrónicos con copia de seguridad.
- Buscar copias de seguridad (la búsqueda de texto completo no es compatible).
- Recuperar copias de seguridad de la nube a la nube a la ubicación original dentro de la organización original de Microsoft 365 o Google Workspace.

Un operador de restauración no puede:

- Eliminar alertas.
- Añadir o eliminar organizaciones de Microsoft 365 o Google Workspace.
- Añadir, eliminar o cambiar el nombre de las ubicaciones de las copias seguridad.
- Eliminar o cambiar el nombre de las copias de seguridad.
- Crear, eliminar o cambiar el nombre de carpetas al recuperar una copia de seguridad a una ubicación personalizada.
- Aplicar un plan de copias de seguridad o ejecutar una copia de seguridad.
- Acceder a los archivos de la copia de seguridad o al contenido de los correos electrónicos con copia de seguridad.
- Descargar archivos de la copia de seguridad o adjuntos de correos electrónicos.
- Enviar recursos en la nube con copia de seguridad, como correos electrónicos o elementos del calendario, mediante correo electrónico.
- Ver o recuperar conversaciones de Microsoft 365 Teams.
- Recuperar copias de seguridad de la nube a la nube a ubicaciones que no sean originales, como un buzón de correo diferente, OneDrive, Google Drive, o Microsoft 365 Team.

Roles de usuario y derechos de la Programación cibernética

Las acciones disponibles con secuencias de comandos y planes de programación dependen del estado de la secuencia de comandos y de su rol de usuario.

Los administradores pueden gestionar objetos en su propio inquilino y en los inquilinos secundarios correspondientes. No pueden ver objetos en un nivel de administración más alto, si los hay, ni acceder a ellos.

Los administradores de nivel inferior tienen acceso de solo lectura a los planes de programación de sus cargas de trabajo a través de un administrador de nivel superior.

Estos roles proporcionan derechos con respecto a la Programación cibernética:

- Administrador de la compañía

Este rol concede todos los derechos de administrador en todos los servicios. Con respecto a la Programación cibernética, concede los mismos derechos que el rol de administrador de cibernética.

- Administrador de cibernética

  Este rol otorga todos los derechos, incluida la aprobación de las secuencias de comandos que pueden utilizarse en el inquilino y la capacidad de ejecutar secuencias de comandos con el estado **Probando**.
- Administrador

  Este rol concede permisos parciales con la capacidad de ejecutar secuencias de comandos aprobadas y de crear y ejecutar planes de programación que utilizan secuencias de comandos aprobadas.
- Administrador de solo lectura

  Este rol concede permisos limitados con la capacidad de ver las secuencias de comandos y los planes de protección que utiliza el inquilino.
- Usuario

  Este rol concede permisos parciales, con la capacidad de ejecutar secuencias de comandos aprobadas y de crear y ejecutar planes de programación que utilizan secuencias de comandos aprobadas, pero solo en el equipo propiedad del usuario.

La siguiente tabla resume todas las acciones disponibles según el estado de la secuencia de comandos y el rol de usuario.

Rol	Objeto	Estado de la secuencia de comandos		
		Borrador	**Probando**	**Aprobado**
Administrador de cibernética Administrador de la compañía	Plan de programación	Editar (Eliminar un borrador de secuencia de comandos de un plan) Eliminarlo Revoque Deshabilitar Detener	Crear Editarlo Aplicar Habilitar Ejecutar Eliminarlo Revoque Deshabilitar Detener	Crear Editarlo Aplicar Habilitar Ejecutar Eliminarlo Revoque Deshabilitar Detener
	Secuencia de comandos	Crear Editarlo Cambiar estado Clonarlo	Crear Editarlo Cambiar estado Ejecutar	Crear Editarlo Cambiar estado Ejecutar

		Eliminarlo Cancelar ejecución	Clonarlo Eliminarlo Cancelar ejecución	Clonarlo Eliminarlo Cancelar ejecución
Administrador Usuario (para sus propias cargas de trabajo)	Plan de programación	Vista Revoque Deshabilitar Detener	Vista Cancelar ejecución	Crear Editarlo Aplicar Habilitar Ejecutar Eliminarlo Revoque Deshabilitar Detener
	Secuencia de comandos	Crear Editarlo Clonarlo Eliminarlo Cancelar ejecución	Vista Clonarlo Cancelar ejecución	Ejecutar Clonarlo Cancelar ejecución
Administrador de solo lectura	Plan de programación	Vista	Vista	Vista
	Secuencia de comandos	Vista	Vista	Vista

Cambiar los ajustes de notificaciones para un usuario

Para cambiar los ajustes de notificaciones para un usuario, vaya a **Gestión empresarial** > **Usuarios**. Seleccione el usuario para el que desee configurar las notificaciones y haga clic en el icono del lápiz en la sección **Configuración**. Están disponibles los siguientes ajustes de notificaciones si el servicio Cyber Protection está habilitado para el inquilino en el que se creó el usuario:

- **Notificaciones de uso excesivo de las cuotas** (habilitado de forma predeterminada)
  Notificaciones sobre cuotas superadas.
- **Informes de uso planificados** (habilitado de forma predeterminada)
  Informes de uso que se envían el primer día de cada mes.

- **Notificaciones de adaptación de marca de URL** (opción deshabilitada de manera predeterminada)
  Notificaciones acerca del próximo vencimiento del certificado utilizado para la URL personalizada de los servicios de Cyber Protect Cloud. Se envían notificaciones a todos los administradores del inquilino seleccionado: 30 días, 15 días, 7 días, 3 días y 1 día antes de que venza el certificado.
- **Notificaciones de error**, **Notificaciones de advertencia** y **Notificaciones de acciones realizadas correctamente** (deshabilitado de forma predeterminada)
  Notificaciones relacionadas con los resultados de la ejecución de planes de protección y con los resultados de las operaciones de recuperación ante desastres de cada dispositivo.
- **Resumen diario de alertas activas** (habilitado de forma predeterminada)
  El resumen diario se genera a partir de la lista de alertas activas presentes en la consola del servicio en el momento de la generación. El resumen se genera y envía una vez al día, entre las 10:00 y las 23:59 UTC. La hora a la que se genera y envía el informe depende de la carga de trabajo del centro de datos. Si no hay alertas activas en ese momento, no se envía el resumen. El resumen no incluye información sobre alertas pasadas que ya no estén activas. Por ejemplo, si un usuario encuentra una copia de seguridad fallida y anula la alerta, o si la copia de seguridad se vuelve a intentar y se completa correctamente antes de generarse el resumen, la alerta ya no estará presente y el resumen no la incluirá.
- **Notificaciones de control de dispositivos** (deshabilitadas de manera predeterminada)
  Notificaciones de los intentos de utilizar dispositivos periféricos y puertos limitados por planes de protección con el módulo de control de dispositivos habilitado.
- **Notificaciones de recuperación** (opción deshabilitada de manera predeterminada)
  Notificaciones sobre las acciones de recuperación en los siguientes recursos: mensajes de correo electrónico del usuario y buzón de correo completo, carpetas públicas; OneDrive/Google Drive: archivos o carpetas completos de OneDrive, archivos de SharePoint; Teams: Canales, todo Teams, mensajes de correo electrónico y sitio de Teams.
  En el contexto de estas notificaciones, se consideran acciones de recuperación las siguientes: enviar un correo electrónico, descargar o iniciar una operación de recuperación.
- **Notificaciones de prevención de pérdida de datos** (opción deshabilitada de manera predeterminada)
  Notificaciones sobre las alertas de prevención de la pérdida de datos relacionadas con la actividad de este usuario en la red.
- **Notificaciones de incidentes de seguridad** (opción deshabilitada de manera predeterminada)
  Notificaciones de malware detectado durante exploraciones en acceso, en ejecución y bajo demanda y de detecciones desde los motores de comportamiento y de filtrado de URL.
  Hay dos opciones disponibles: **Mitigado** y **No mitigado**. Estas opciones son relevantes para las alertas de incidentes de Detección y respuesta de endpoints (EDR), las alertas EDR de fuente de amenazas y las alertas individuales (para las cargas de trabajo que no tienen activada la EDR).
  Cuando se crea una alerta EDR, se envía un correo electrónico al usuario correspondiente. Si el estado de la amenaza del incidente cambia, se envía un nuevo correo electrónico. Los correos electrónicos incluyen botones de acción que permiten al usuario ver detalles del incidente (si se ha mitigado) o investigar y solucionar el incidente (si no se ha mitigado).

- **Notificaciones de infraestructura** (deshabilitadas de forma predeterminada)
  Notificaciones sobre problemas con la infraestructura de la recuperación ante desastres: cuando la infraestructura de la recuperación ante desastres o los túneles VPN no están disponibles.

Todas las notificaciones se envían a la dirección de correo electrónico del usuario.

Notificaciones recibidas por cada función de usuario

Las notificaciones que Cyber Protection envía dependen de la función de usuario.

Tipo de notificación/función de usuario	Usuario	Administrador de clientes
Notificaciones de los dispositivos propios	Sí	Sí
Notificaciones de todos los dispositivos de la organización	n/d	Sí (excepto **Notificaciones de incidentes de seguridad**)
Notificaciones de Microsoft 365, Google Workspace y otras copias de seguridad basadas en la nube	n/d	Sí

Tipo de notificación/función de usuario	Usuario	Administradores de clientes y unidades	Administrador de socios y carpetas
Notificaciones de los dispositivos propios	Sí	Sí	n/d*
Notificaciones de todos los dispositivos de los inquilinos secundarios	n/d	Sí	Sí
Notificaciones de Microsoft 365, Google Workspace y otras copias de seguridad basadas en la nube	n/d	Sí	Sí

* Los administradores de socios no pueden registrar sus propios dispositivos, pero sí crear sus propias cuentas de administrador de clientes y utilizarlas para agregar sus dispositivos propios. Consulte Cuentas de usuario e inquilinos.

Deshabilitación y habilitación de una cuenta de usuario

Es posible que tenga que deshabilitar una cuenta de usuario para restringir temporalmente su acceso a la plataforma en la nube.

Pasos para deshabilitar una cuenta de usuario

1. En el portal de administración, vaya a **Usuarios**.
2. Seleccione la cuenta de usuario que desee deshabilitar y, a continuación, haga clic en el icono > **Deshabilitar**.
3. Haga clic en **Deshabilitar** para confirmar la acción.

Como resultado, este usuario no podrá usar la plataforma en la nube ni recibir ninguna notificación.

Para habilitar una cuenta de usuario deshabilitada, selecciónela de la lista de usuarios y, a continuación, haga clic en el icono > **Habilitar**.

Eliminación de una cuenta de usuario

Es posible que tenga que eliminar una cuenta de usuario permanentemente para liberar los recursos que usa, como espacio de almacenamiento o licencia. Las estadísticas de uso se actualizarán en el plazo de un día después de la eliminación. En cuentas con muchos datos, es posible que tarde más.

Antes de eliminar una cuenta de usuario, tiene que deshabilitarla. Para obtener más información sobre cómo hacerlo, consulte: Deshabilitación y habilitación de una cuenta de usuario.

Importante
La eliminación de una cuenta de usuario es una acción irreversible.

Pasos para eliminar una cuenta de usuario

1. En el portal de administración, vaya a **Usuarios**.
2. Seleccione la cuenta de usuario deshabilitada y, a continuación, haga clic en el icono de puntos suspensivos > **Eliminar**.
3. Para confirmar su acción, introduzca su información de inicio de sesión y luego haga clic en **Eliminar**.

Como resultado:

- Se eliminará esta cuenta de usuario.
- Se eliminarán todos los datos que pertenecen a esta cuenta de usuario.
- Se eliminará el registro de todos los equipos asociados a esta cuenta de usuario.

Transferencia de la propiedad de una cuenta de usuario

Es posible que tenga que transferir la propiedad de una cuenta de usuario si quiere conservar el acceso a los datos de un usuario restringido.

Importante
No se puede reasignar el contenido de una cuenta eliminada.

Pasos para transferir la propiedad de una cuenta de usuario:

1. En el portal de administración, vaya a **Usuarios**.
2. Seleccione la cuenta de usuario cuya propiedad quiera transferir y, a continuación, haga clic en el icono del lápiz de la sección **información general**.

3. Sustituya el correo electrónico existente por el del futuro propietario de la cuenta y luego haga clic en **Listo**.
4. Haga clic en **Sí** para confirmar la acción.
5. Deje que el futuro propietario de la cuenta compruebe su dirección de correo electrónico siguiendo las instrucciones que se le han enviado por esa vía.
6. Seleccione la cuenta de usuario cuya propiedad está transfiriendo y luego haga clic en el icono > **Restablecer contraseña**.
7. Haga clic en **Restablecer** para confirmar la acción.
8. Deje que el futuro propietario de la cuenta restablezca la contraseña siguiendo las instrucciones que se le han enviado a su dirección de correo electrónico.

Ahora el nuevo usuario puede acceder a esta cuenta.

Establecimiento de la autenticación de doble factor

La **autenticación de doble factor** es un tipo de autenticación de varios factores que comprueba la identidad de un usuario mediante la combinación de dos factores distintos:

- Algo que un usuario conoce (PIN o contraseña).
- Algo que un usuario posee (token).
- Algo que un usuario es (biometría).

La autenticación de doble factor proporciona protección adicional contra el acceso no autorizado a su cuenta.

La plataforma es compatible con la autenticación por **contraseña de un solo uso y duración definida (TOTP)**. Si se activa la autenticación TOTP en el sistema, los usuarios deben introducir su contraseña habitual y el código TOTP de un solo uso para acceder al sistema. Dicho de otro modo, el usuario introduce la contraseña (el primer factor) y el código TOTP (el segundo factor). El código TOTP se genera en la aplicación de autenticación del dispositivo de segundo factor del usuario, basándose en la hora actual y el código secreto (QR o alfanumérico) que proporciona la plataforma.

Cómo funciona

1. Puede habilitar la autenticación de doble factor a nivel de su organización.
2. Todos los usuarios de su organización deben instalar una aplicación de autenticación en sus dispositivos de segundo factor (teléfonos móviles, equipos portátiles, de sobremesa o tabletas). Dicha aplicación se utilizará para generar códigos TOTP de un solo uso. Aplicaciones de autenticación recomendadas:
   - Google Authenticator

     Versión de la aplicación de iOS (https://apps.apple.com/app/google-authenticator/id388497605)

Versión de Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)

- Microsoft Authenticator

  Versión de la aplicación de iOS (https://apps.apple.com/app/microsoft-authenticator/id983156458)

  Versión de Android (https://play.google.com/store/apps/details?id=com.azure.authenticator)

Importante
Los usuarios deben establecer correctamente la hora en el dispositivo en el que instalen la aplicación de autenticación, de forma que refleje la hora actual.

3. Los usuarios de su organización deben volver a iniciar sesión en el sistema.
4. Tras introducir la información de inicio de sesión y la contraseña, se les solicitará que establezcan la autenticación de doble factor para su cuenta de usuario.
5. Deben escanear el código QR con su aplicación de autenticación. Si no pueden escanear el código QR, pueden usar el código secreto TOTP que aparece bajo el código QR y agregarlo manualmente en la aplicación de autenticación.

Importante
Se recomienda guardarlo (imprimir el código QR, escribir el código secreto TOTP o usar una aplicación compatible con la creación de copias de seguridad de códigos en la nube). Necesitará el código secreto TOTP para restablecer la autenticación de doble factor en caso de perder el dispositivo de segundo factor.

6. El código TOTP de un solo uso se generará en la aplicación de autenticación. Se regenera automáticamente cada 30 segundos.
7. Los usuarios deben introducir el código TOTP en la pantalla "Establecer autenticación de doble factor" después de introducir la contraseña.
8. Como resultado, se establecerá la autenticación de doble factor para los usuarios.

Cuando los usuarios inicien sesión en el sistema, se les solicitará la información de inicio de sesión, la contraseña y el código TOTP de un solo uso generado en la aplicación de autenticación. Al iniciar sesión en el sistema, los usuarios pueden establecer que su navegador es de confianza y no se les volverá a solicitar el código TOTP las próximas veces que inicien sesión en dicho navegador.

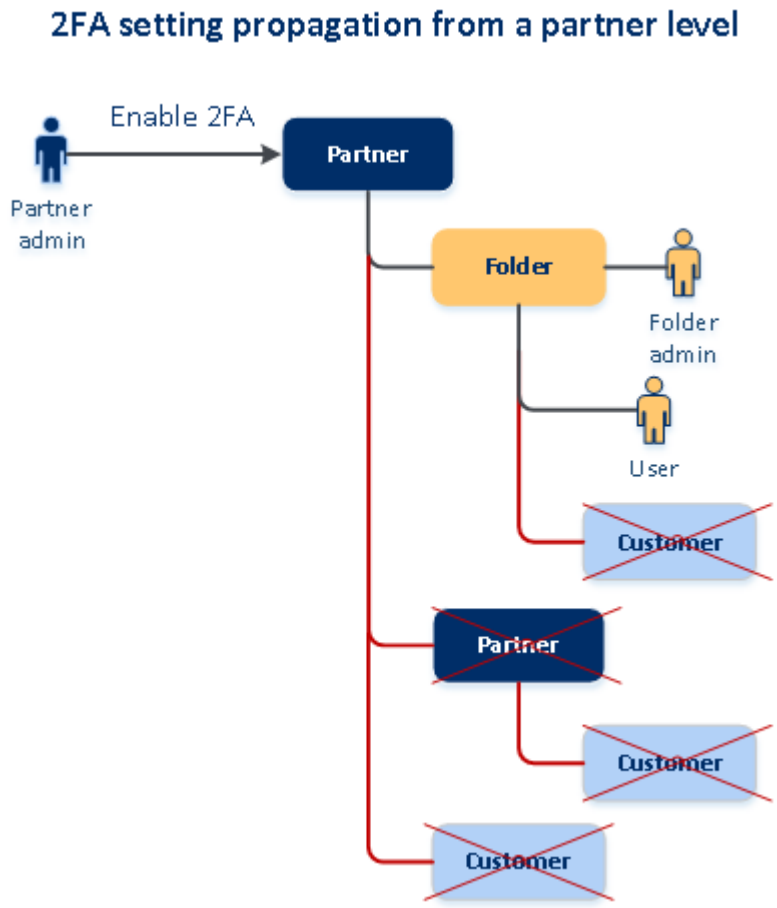
Propagación de la configuración de doble factor en niveles de inquilino

La autenticación de doble factor se establece en el nivel de **organización**. Usted puede habilitar o deshabilitar la autenticación de doble factor:

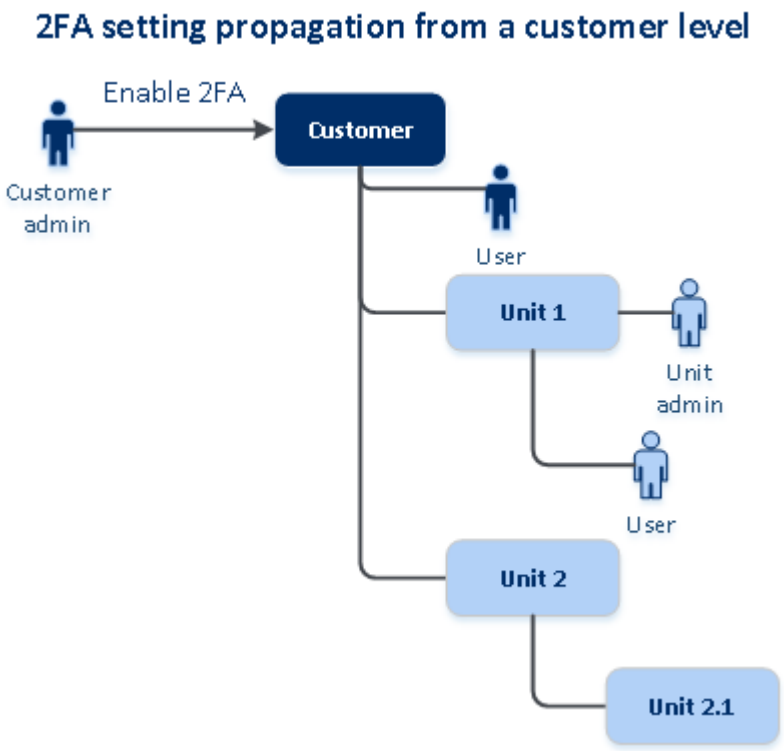
- Para su propia organización.
- Para su inquilino secundario (solo en caso de que la opción **Acceso al soporte técnico** esté habilitada en ese inquilino secundario).

La configuración de la autenticación de doble factor se propaga a los niveles de inquilino de la siguiente manera:

- Las carpetas heredan automáticamente la configuración de autenticación de doble factor de la organización de sus socios. En el siguiente esquema, las líneas rojas indican que no es posible la propagación de la configuración de autenticación de doble factor.



- Las unidades heredan automáticamente la configuración de autenticación de doble factor de la organización de sus clientes.



Nota

1. Puede habilitar la autenticación de doble factor en sus organizaciones secundarias solo si la opción **Acceso al soporte técnico** está habilitada en esa organización secundaria.
2. Puede gestionar la configuración de autenticación de doble factor de los usuarios de las organizaciones secundarias solo si la opción **Acceso al soporte técnico** está habilitada en esa organización secundaria.
3. No es posible establecer la autenticación de doble factor en el nivel de unidad o carpeta.
4. Puede configurar la autenticación de doble factor aunque su organización principal no tenga esta configuración habilitada.

Establecimiento de la autenticación de doble factor para el inquilino

Como administrador, puede habilitar la autenticación de dos factores para la organización.

Para habilitar la autenticación de doble factor para el inquilino:

1. En el portal de gestión, vaya a **Configuración** > **Seguridad**.
2. Active el control deslizante **Autenticación de dos factores** y haga clic en **Habilitar**.

Ahora todos los usuarios de la organización deben establecer la autenticación de dos factores en sus cuentas. Se les solicitará que lo hagan la próxima vez que intenten iniciar sesión o cuando sus sesiones actuales caduquen.

La barra de progreso bajo el control deslizante muestra cuántos usuarios han establecido la autenticación de dos factores para sus cuentas. Para comprobar que los usuarios hayan

configurado sus cuentas, acceda a la pestaña **Gestión empresarial** > **Usuarios** y consulte la columna **Estado de la autenticación de doble factor**. El estado de 2FA de los usuarios que no hayan configurado la autenticación de dos factores en la cuenta será **Configuración requerida**.

Tras configurar correctamente la autenticación de dos factores, los usuarios deberán introducir su nombre de usuario, contraseña y un código TOTP cada vez que inicien sesión en la consola de servicio.

Para deshabilitar la autenticación de doble factor para el inquilino:

1. En el portal de gestión, vaya a **Configuración** > **Seguridad**.
2. Para deshabilitar la autenticación de dos factores, desactive el control deslizante y haga clic en **Deshabilitar**.
3. [Si al menos un usuario ha configurado la autenticación de doble factor dentro de la organización] Introduzca el código TOTP generado en su aplicación de autenticación del dispositivo móvil.

Como resultado, se deshabilita la autenticación de doble factor en su organización, se eliminan todos los secretos y se borran todos los navegadores de confianza. Todos los usuarios iniciarán sesión en el sistema usando únicamente su información de inicio de sesión y contraseña. En la pestaña **Gestión empresarial** > **Usuarios**, se ocultará la columna **Estado de la autenticación de doble factor**.

Gestión de la autenticación de doble factor para usuarios

Puede controlar la configuración de la autenticación de doble factor para todos sus usuarios y restablecerla en el portal de administración, en la pestaña **Gestión empresarial** > **Usuarios**.

Supervisión

En el portal de administración, en **Gestión empresarial** > **Usuarios**, puede ver una lista de los usuarios de su organización. El **estado de la autenticación de doble factor** indica si se ha establecido la configuración de doble factor para un usuario.

Pasos para restablecer la autenticación de doble factor para un usuario

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. En la pestaña **Usuarios** , busque el usuario cuya configuración desee cambiar y haga clic en el icono de elipsis.
3. Haga clic en **Restablecer autenticación de doble factor**.
4. Introduzca el código TOTP generado en la aplicación de autenticación del dispositivo de segundo factor y haga clic en **Restablecer**.

Como resultado, el usuario podrá volver a establecer la autenticación de doble factor.

Para restablecer los navegadores de doble confianza para un usuario:

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. En la pestaña **Usuarios** , busque el usuario cuya configuración desee cambiar y haga clic en el icono de elipsis.
3. Haga clic en **Restablecer todos los navegadores de confianza**.
4. Introduzca el código TOTP generado en la aplicación de autenticación del dispositivo de segundo factor y haga clic en **Restablecer**.

El usuario para el que ha restablecido todos los navegadores de confianza tendrá que proporcionar el código TOTP la próxima vez que inicie sesión.

Los usuarios pueden restablecer tanto los navegadores de confianza como la configuración de autenticación de doble factor por sí mismos. Para ello, deben iniciar sesión en el sistema haciendo clic en el enlace correspondiente e introduciendo el código TOTP para confirmar la operación.

Para deshabilitar la autenticación de doble factor para un usuario:

No recomendamos que deshabilite la autenticación de doble factor porque genera la posibilidad de que aparezcan amenazas de la seguridad del inquilino.

Como excepción, puede deshabilitar la autenticación de doble factor para un usuario y mantenerla para el resto de usuarios del inquilino. Es una solución para los casos en los que la autenticación de doble factor está habilitada en un inquilino en el que hay una integración de la nube configurada y esta integración da autorización a la plataforma mediante la cuenta del usuario (nombre de usuario y contraseña). Para seguir usando la integración, como solución temporal, se puede convertir el usuario en una cuenta de servicio que no admita autenticación de doble factor.

Importante
No se recomienda cambiar usuarios comunes a usuarios del servicio para deshabilitar la autenticación de doble factor porque implica riesgos para la seguridad del inquilino.

Para usar integraciones de la nube sin deshabilitar la autenticación de doble factor de los inquilinos, la solución segura que se recomienda es crear clientes API y configurar sus integraciones de cloud para que funcionen con ellas.

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. En la pestaña **Usuarios** , busque el usuario cuya configuración desee cambiar y haga clic en el icono de elipsis.
3. Haga clic en **Marcar como cuenta de servicio**. Como resultado, un usuario obtendrá un estado de autenticación de doble factor especial llamado **Cuenta de servicio.**
4. [Si al menos un usuario dentro de un inquilino ha configurado la autenticación de doble factor] Introduzca el código TOTP generado en la aplicación de autenticación del dispositivo de segundo factor para confirmar la desactivación.

Para habilitar la autenticación de doble factor para un usuario:

Puede tener que habilitar la autenticación de doble factor para un usuario específico para el que la había deshabitado anteriormente.

1. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
2. En la pestaña **Usuarios** , busque el usuario cuya configuración desee cambiar y haga clic en el icono de elipsis.
3. Haga clic en **Marcar como cuenta habitual**. Como resultado, el usuario tendrá que establecer la autenticación de doble factor o introducir el código TOTP al entrar en el sistema.

Restablecimiento de la autenticación de doble factor en caso de pérdida de dispositivo de segundo factor

Para restablecer el acceso a su cuenta en caso de haber perdido el dispositivo de segundo factor, siga una de estas sugerencias:

- Restaure su código secreto TOTP (código QR o alfanumérico) a partir de una copia de seguridad. Use otro dispositivo de segundo factor y agregue el código secreto TOTP guardado en la aplicación de autenticación instalada en dicho dispositivo.
- Pida a su administrador que restablezca la configuración de autenticación de doble factor para usted.

Protección de fuerza bruta

Un ataque de fuerza bruta es aquel en el que un intruso intenta acceder al sistema mediante el uso de numerosas contraseñas con la esperanza de que una de ellas sea la correcta.

La plataforma cuenta con un sistema de protección contra la fuerza bruta que se basa en cookies del dispositivo.

La configuración predeterminada de la plataforma para la protección contra la fuerza bruta es la siguiente:

Parámetro	Ingresar la mot de passe	Introducción del código TOTP
Límite de intentos	10	5
Período límite de intentos (el límite se restablece después del tiempo de espera)	15 min (900 s)	15 min (900 s)
Momento del bloqueo	Límite de intentos + 1 (11.º intento)	Límite de intentos
Período de bloqueo	5 min (300 s)	5 min (300 s)

Si habilita la autenticación de doble factor, se emite una cookie del dispositivo a un cliente (navegador) una vez que la autenticación se ha efectuado correctamente mediante ambos factores (contraseña y código TOTP).

En el caso de los navegadores de confianza, la cookie del dispositivo se emite tras una autenticación correcta mediante un solo factor (contraseña).

Los intentos de introducción del código TOTP se registran por usuario, no por dispositivo. Esto significa que, aunque un usuario intente introducir el código TOTP en varios dispositivos, estos se bloquearán igualmente.

Configuración de situaciones relacionadas con la venta de productos de gama superior a sus clientes

La venta de productos de gama superior es una técnica para invitar a sus clientes a adquirir características adicionales.

Cyber Protection tiene varias ediciones heredadas, cuyas funciones y precios son diferentes. Es posible que quiera promocionar ediciones más caras con funciones más avanzadas para sus clientes existentes que usan ediciones básicas.

Puede habilitar o deshabilitar la capacidad de venta de productos de gama superior para cada cliente. De forma predeterminada, la opción de venta de productos de gama superior está desactivada. Si habilita la venta de productos de gama superior para un cliente, verá la funcionalidad adicional, pero no estará disponible hasta que el cliente adquiera la edición promocionada. Esta funcionalidad adicional se marca con etiquetas en las que aparece el nombre o los iconos de la edición promocionada, todo destacado en naranja. Estos puntos de venta de productos de gama superior se mostrarán a un cliente para motivarle a adquirir una edición más cara. Al hacer clic en estos puntos de venta de productos de gama superior, el cliente verá un cuadro de diálogo en el que se le sugerirá que adquiera una edición más cara para habilitar la funcionalidad deseada.

El elemento de acción depende del tipo de usuario cliente. El tipo de usuario (comprador o no comprador) se puede configurar utilizando la API de la plataforma. Para obtener más información, consulte la documentación sobre la API. Si necesita más información sobre los elementos de acción que se muestran a sus clientes, consulte esta tabla:

Tipo de usuarios en inquilino cliente	Elemento de acción
Administrador; comprador	El botón **Comprar ahora** aparece en la interfaz de usuario.*
Administrador; no comprador	En la interfaz de usuario aparece el mensaje "Póngase en contacto con el partner para actualizar la edición".
Usuario; comprador	En la interfaz de usuario aparece el mensaje "Póngase en contacto con el partner para actualizar la edición".

Usuario; no comprador	En la interfaz de usuario aparece el mensaje "Póngase en contacto con el partner para actualizar la edición".

***** El enlace del botón **Comprar ahora**, que redirigirá al cliente a un sitio web para que adquiera una edición más avanzada, se puede configurar en **Configuración**> **Personalización de marca**. En la sección **Venta de productos de gama superior**, puede especificar **URL de compra**. Las opciones de personalización de la marca se aplicarán a todos los partners o carpetas directos o indirectos secundarios, y a los clientes del inquilino donde se configure la personalización de la marca.

Pasos para habilitar o deshabilitar la capacidad de venta de productos de gama superior para un cliente

1. En el portal de gestión, vaya a **Clientes**.
2. Seleccione el cliente, vaya al panel de la derecha y haga clic en la pestaña **Configurar**.
3. En la sección **Venta de productos de gama superior**, haga lo siguiente:
   - Habilite la opción **Promocionar ediciones más avanzadas** para activar la venta de productos de gama superior para el cliente.
   - Deshabilite la opción **Promocionar ediciones más avanzadas** para desactivar la venta de productos de gama superior para el cliente.

Puntos de venta de productos de gama superior que se muestran a un cliente

Lista de vulnerabilidades

En la consola de servicio, puede encontrar la lista de vulnerabilidades en **Gestión del software** > **Vulnerabilidades**. Cuando un usuario haga clic en el icono de puntada, se abrirá un cuadro de diálogo con la promoción de la edición para incitar al usuario a adquirir la edición más cara.

Crear o editar un plan de protección

En la consola de servicio, esta opción se encuentra en **Planes** > **Protección**. Haga clic en **Crear plan**. En las ediciones de Cyber Backup solo están habilitados los módulos **Copia de seguridad** y **Vulnerabilidad**. El resto de los módulos únicamente están disponibles en las ediciones de Cyber Protect. Su cliente tendrá todos los módulos habilitados cuando adquiera una de las ediciones de Cyber Protect.

Asistente para la autodetección

En la consola de servicio, este asistente se encuentra en **Dispositivos** > **Todos los dispositivos**. Para que su cliente pueda iniciar el asistente de autodetección, tendrá que hacer clic en **Añadir**, acceder a la sección **Varios dispositivos** y, por último, hacer clic en **Solo Windows**. Los métodos de detección de equipos automáticos estarán disponibles únicamente en las ediciones avanzadas.

Acciones de la lista de dispositivos

En la consola de servicio, esta lista se encuentra en **Dispositivos** > **Todos los dispositivos**. Su cliente debe seleccionar el equipo y, a continuación, aparecerán dos opciones adicionales en el panel de la izquierda:

- **Conectar mediante cliente HTML5**
- **Parche**

Estas opciones estarán disponibles únicamente si el cliente adquiere una edición más cara que la que tiene.

Gestión de ubicaciones y almacenamiento

La sección **Configuración** > **Ubicaciones** muestra los almacenamientos en la nube y las infraestructuras de recuperación ante desastres que puede utilizar para proporcionar los servicios **Cyber Protection** y **File Sync & Share** a sus partners y clientes.

Los almacenamientos configurados para otros servicios se mostrarán en la sección **Ubicaciones** en próximas versiones.

Ubicaciones

Una ubicación es un contenedor que le sirve para agrupar cómodamente los almacenamientos en el cloud y las infraestructuras de recuperación ante desastres. Puede representar cualquier cosa que desee, como un centro de datos específico o una ubicación geográfica de los componentes de su infraestructura.

Puede crear todas las ubicaciones que quiera y llenarlas con almacenamientos de copia de seguridad, infraestructuras de recuperación ante desastres y almacenamientos de **File Sync & Share**. En una ubicación puede haber varios almacenamientos en el cloud, pero solo una infraestructura de recuperación ante desastres.

Para obtener información sobre las operaciones que se pueden llevar a cabo con los almacenamientos, consulte "Gestión de almacenamiento".

Selección de ubicaciones y almacenamientos para socios y clientes

Al crear un inquilino socio/carpeta, puede seleccionar diversas ubicaciones y varios almacenamientos que estarán disponibles en el inquilino nuevo para cada servicio.

Al crear un inquilino cliente, tiene que seleccionar una ubicación y, luego, un almacenamiento por servicio dentro de esta ubicación. Los almacenamientos asignados al cliente se pueden cambiar más adelante, pero únicamente si su uso es 0 GB, es decir, antes de que el cliente empiece a usarlos o después de que el cliente elimine todas las copias de seguridad de ese almacenamiento.

La información sobre los almacenamientos asignados a un inquilino de cliente se muestra en el panel de detalles del inquilino cuando se selecciona en la pestaña **Clientes**. La información sobre el uso del espacio de almacenamiento no se actualiza en tiempo real. Por favor, espere 24 horas para que la información se actualice.

Operaciones con ubicaciones

Para crear una nueva ubicación, haga clic en **Añadir ubicación** y después especifique el nombre de la ubicación.

Para mover un almacenamiento o una infraestructura de recuperación ante desastres a otra ubicación, seleccione el almacenamiento o la infraestructura, haga clic en el icono de lápiz del campo **Ubicación** y seleccione la ubicación de destino.

Para cambiar el nombre de una ubicación, haga clic en el icono de puntos suspensivos que se encuentra junto a su nombre y, luego, en **Cambiar nombre**. Por último, especifique el nuevo nombre de la ubicación.

Para eliminar una ubicación, haga clic en el icono de puntos suspensivos que se encuentra junto a su nombre y, luego, en **Eliminar**. Por último, confirme su decisión. Solo se pueden eliminar las ubicaciones vacías.

Gestión de almacenamiento

Agregar almacenamientos nuevos

- Servicio **Cyber Protection** :
  - De forma predeterminada, los almacenamientos de copias de seguridad se encuentran en los centros de datos de .
  - Si un administrador de un nivel superior ha habilitado el artículo de oferta de **almacenamiento de copias de seguridad del partner** para un inquilino del socio, los administradores del socio pueden organizar el almacenamiento en el centro de datos propio del socio mediante el uso del software de Cyber Infrastructure de . Haga clic en **Añadir almacenamiento de copia de seguridad** en la sección **Ubicaciones** para obtener información sobre cómo organizar un almacenamiento de copias de seguridad en su propio centro de datos.
  - Si un administrador de un nivel superior ha habilitado la **infraestructura de recuperación ante desastres del socio** que ofrece el elemento para el inquilino del socio, los administradores del socio pueden organizar la infraestructura de recuperación ante desastres del socio en el centro de datos propio del socio. Para obtener información sobre cómo añadir una infraestructura de recuperación ante desastres, póngase en contacto con el soporte técnico.

Nota
La validación de la copia de seguridad no es posible con almacenamientos de objetos en la nube pública, como Amazon S3, Microsoft Azure, Google Cloud Storage y Wasabi, empleados por los centros de datos de .
La validación de la copia de seguridad es posible con almacenamientos de objetos en la nube pública empleados por los partners de . Sin embargo, no se recomienda habilitarlo, porque las operaciones de validación aumentan el tráfico de salida desde esos almacenamientos de objetos públicos y pueden ocasionar gastos importantes.

- Para obtener información sobre cómo añadir almacenamientos que utilizarán otros servicios, póngase en contacto con el soporte técnico.

Eliminación de almacenamientos

Puede eliminar almacenamientos que haya añadido usted o sus inquilinos secundarios.

Si el almacenamiento está asignado a algún inquilino de cliente, debe deshabilitar el servicio que use el almacenamiento para todos los inquilinos cliente antes de eliminar el almacenamiento.

Pasos para eliminar un almacenamiento

1. Inicie sesión en el portal de gestión.
2. Vaya hasta el inquilino al que se haya añadido el almacenamiento.
3. Haga clic en **Configuración** > **Ubicaciones**.
4. Seleccione el almacenamiento que desee eliminar.
5. En el panel de propiedades de almacenamiento, haga clic en el icono de elipsis y, a continuación, haga clic en **Eliminar almacenamiento**.
6. Confirme su decisión.

Configuración del almacenamiento inmutable

Puede configurar el almacenamiento inmutable en el nivel de partner y de cliente.

Para los inquilinos partner, no hay una selección de modos de almacenamiento inmutables. Un administrador puede deshabilitar y volver a habilitar el almacenamiento inmutable, así como cambiar el modo y el período de retención.

Para los inquilinos cliente, el almacenamiento inmutable está disponible en los siguientes modos:

- **Modo de gobierno**
  En este modo, un administrador puede deshabilitar y volver a habilitar el almacenamiento inmutable, así como cambiar el modo y el período de retención.
- **Modo de cumplimiento normativo**
  Después de seleccionar este modo, el almacenamiento inmutable no puede deshabilitarse y ya no se puede cambiar el modo o período de retención.

Cuando no se aplica ninguna configuración personalizada a un inquilino secundario, este hereda la del principal.

Solo se puede configurar la configuración del almacenamiento inmutable si está habilitada la autenticación de doble factor para el inquilino al que pertenece la cuenta de administrador.

Las copias de seguridad eliminadas del almacenamiento inmutable siguen utilizando el espacio de almacenamiento y se facturan según corresponda.

Nota
A partir de la versión 21.12, a los nuevos inquilinos de tipo partner se les habilita de forma predeterminada un almacenamiento inmutable con un período de retención de 14 días. Los inquilinos existentes deben habilitar el almacenamiento inmutable de forma manual.

Pasos para habilitar el almacenamiento inmutable para un inquilino partner

1. Inicie sesión en el portal de administración como administrador y vaya a **Configuración** > **Seguridad**.
2. Habilite el control deslizante **Almacenamiento inmutable**.
3. Especifique un período de retención de entre 14 y 999 días.
   El período de retención predeterminado es de 14 días. Si establece un período de retención mayor, puede aumentar el uso del almacenamiento.
4. Haga clic en **Guardar**.

Pasos para deshabilitar el almacenamiento inmutable para un inquilino partner

1. Inicie sesión en el portal de administración como administrador y vaya a **Configuración** > **Seguridad**.
2. Deshabilite el control deslizante **Almacenamiento inmutable**.

   Advertencia.
   Este cambio lo heredarán todos los inquilinos secundarios que no utilizan una configuración personalizada para el almacenamiento inmutable. Todas las copias de seguridad borradas se eliminarán permanentemente. La eliminación de las nuevas copias de seguridad también será permanente.

3. Haga clic en **Deshabilitar** para confirmar su elección.

Pasos para habilitar el almacenamiento inmutable para un inquilino cliente

1. Inicie sesión en el portal de administración como administrador y vaya a **Clientes**.
2. Para editar la configuración de un inquilino cliente, haga clic en su nombre.
3. En el menú de navegación, vaya a **Configuración** > **Seguridad**.
4. Habilite el control deslizante **Almacenamiento inmutable**.
5. Especifique un período de retención de entre 14 y 999 días.

El período de retención predeterminado es de 14 días. Si establece un período de retención mayor, puede aumentar el uso del almacenamiento.

6. Seleccione el modo de almacenamiento inmutable.

   Advertencia.
   La selección del **Modo de cumplimiento normativo** es irreversible. Ya no puede deshabilitar el almacenamiento inmutable ni puede cambiar su modo o período de retención.

7. Haga clic en **Guardar**.

Pasos para deshabilitar el almacenamiento inmutable para un inquilino cliente

1. Inicie sesión en el portal de administración como administrador y vaya a **Clientes**.
2. Para editar la configuración de un inquilino cliente, haga clic en su nombre.
3. En el menú de navegación, vaya a **Configuración** > **Seguridad**.
4. Deshabilite el control deslizante **Almacenamiento inmutable**.

   Nota
   Solo puede deshabilitar el almacenamiento inmutable en el modo de gobierno.

   Advertencia.
   Si deshabilita el almacenamiento inmutable, todas las copias de seguridad borradas se eliminarán permanentemente. La eliminación de las nuevas copias de seguridad también será permanente.

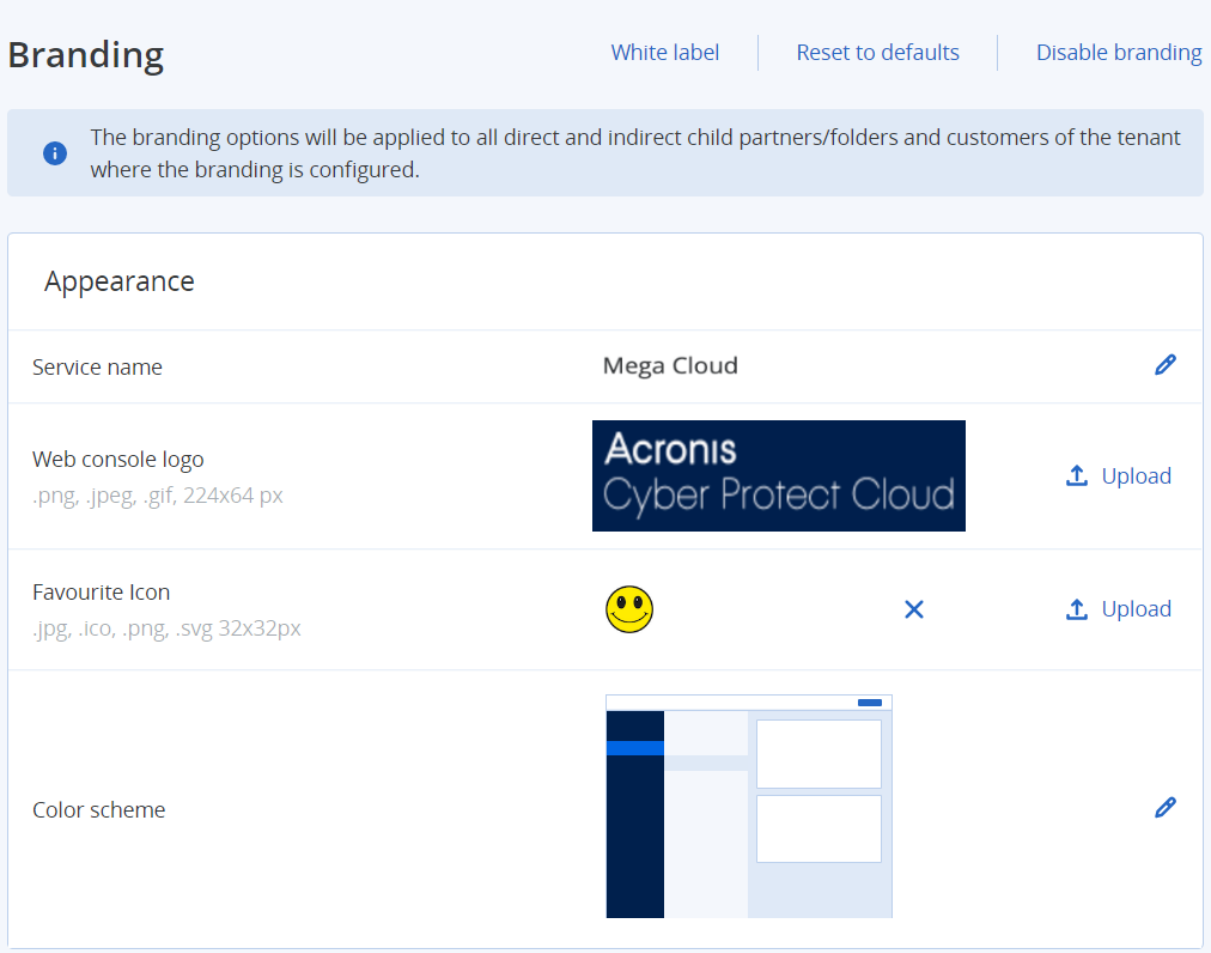
5. Haga clic en **Deshabilitar** para confirmar su elección.

Limitaciones

- El almacenamiento inmutable está disponible con almacenamiento alojados por Acronis o partners que usen Acronis Cyber Infrastructure versión 4.7.1 o posteriores.
  El almacenamiento inmutable requiere que el puerto TCP 40440 esté abierto para el servicio de Backup Gateaway en Acronis Cyber Infrastructure. En las versiones 4.7.1 y posteriores, el puerto TCP 40440 se abre automáticamente con el tipo de tráfico **Copia de seguridad (ABGW) pública**. Para obtener más información sobre los tipos de tráfico, consulte la documentación de Acronis Cyber Infrastructure.
- Para el almacenamiento inmutable es necesario un agente de protección versión 21.12 (compilación 15.0.28532) o posteriores.
- Solo se admiten copias de seguridad TIBX (versión 12).

Configuración de personalización de marca y etiquetado en blanco

La sección **Configuración** > **Personalización de marca** permite a los administradores de partners personalizar la interfaz de usuario del portal de administración y del servicio **Cyber Protection** para eliminar cualquier asociación con los partners de nivel superior.



La personalización de marca se puede configurar en los niveles de carpeta y socio. La personalización de la marca se aplica a todos los socios o carpetas directos o indirectos secundarios y a los clientes del inquilino donde se configure la personalización de la marca.

Otros servicios proporcionan capacidades de personalización de marca independientes en sus consolas de servicio. Para obtener más información, consulte las guías del usuario de los servicios correspondientes.

Elementos de personalización de marca

Apariencia

- **Nombre del servicio**. Este nombre se utiliza en todos los mensajes de correo electrónico que se envían mediante el portal de gestión y los servicios en la nube (mensajes de activación de cuenta y mensajes de correo electrónico de notificaciones de servicio), en la pantalla de **bienvenida** tras el primer inicio de sesión y como nombre de la pestaña del navegador del portal de gestión.
- **Logotipo de la consola web**. El logotipo se muestra en el portal de gestión y en los servicios. Haga clic en **Cargar** para cargar un archivo de imagen.
- **Icono favorito** [Disponible solo si se ha configurado una URL personalizada]. Se muestra el favicon junto al título de la página en la pestaña del navegador. Haga clic en **Cargar** para cargar un archivo de imagen.
- **Esquema de colores** El esquema de colores define la combinación de colores que se utiliza para todos los elementos de interfaz de usuario.

Nota
Haga clic en **Vista previa del esquema en una nueva pestaña** para ver el aspecto de su interfaz para sus inquilinos secundarios. La personalización de la marca no se aplicará hasta que haga clic en **Listo** en el panel **Elegir esquema de colores**.

Personalización de marca del agente y el programa de instalación

Puede modificar la personalización de marca de los archivos de instalación del agente y de Tray Monitor para Windows y macOS.

Nota
Para habilitar esta funcionalidad de personalización de marca, debe actualizar los agentes de Cyber Protection a la versión 15.0.28816 (con fecha de lanzamiento en 01/22) o a una versión posterior.

- **Nombre de archivo del programa de instalación del agente**. Nombre del archivo de instalación que se descarga en cargas de trabajo protegidas.
- **Logotipo del programa de instalación del agente**. Logotipo que se muestra en el asistente de configuración durante la instalación del agente. Haga clic en **Cargar** para cargar un archivo de imagen.
- **Nombre del agente**. Nombre que se muestra en el asistente de configuración durante la instalación del agente.
- **Nombre de Tray Monitor**. Nombre que se muestra en la parte superior de la ventana de Tray Monitor.

Documentación y soporte técnico

- **URL de inicio** Este página se abre cuando un usuario hace clic en el nombre de la empresa en el panel **Acerca de**.
- **URL del soporte técnico**. Este página se abre cuando un usuario hace clic en el enlace **Contactar con el soporte técnico** en el panel **Acerca de** o en un mensaje de correo electrónico enviado mediante el portal de gestión.
- **Teléfono de soporte técnico**. Este número de teléfono se muestra en el panel **Acerca de**.
- **URL de la base de conocimientos**. Este página se abre cuando un usuario hace clic en el enlace **Base de conocimientos** en un mensaje de error.
- **Guía del administrador del portal de administración**. Esta página se abre cuando un usuario hace clic en el icono de interrogación situado en la esquina superior derecha de la interfaz de usuario del portal de administración y, a continuación, hace clic en **Acerca de** > **Manual del administrador**.
- **Ayuda del administrador del portal de administración**. Esta página se abre cuando un usuario hace clic en el icono de interrogación situado en la esquina superior derecha de la interfaz de usuario del portal de administración y, a continuación, hace clic en **Ayuda**.

URL para los servicios de Cyber Protect Cloud

Puede hacer que los servicios de Cyber Protect Cloud estén disponibles desde su dominio personalizado. Haga clic en **Configurar** para establecer una URL personalizada por primera vez, o haga clic en **Reconfigurar** para cambiar la existente. Para utilizar la URL predeterminada (https://cloud.acronis.com), haga clic en **Restablecer valores predeterminados**. Para obtener más información sobre las URL personalizadas, consulte "Configuración de URL de la interfaz web personalizadas".

Configuración de documentos legales

- **URL del Acuerdo de licencia para el usuario final (EULA)**. Esta página se abre cuando un usuario hace clic en el enlace **Acuerdo de licencia para el usuario final** en el panel **Acerca de** o en la pantalla de **Bienvenida** después del primer inicio de sesión, y en las páginas de destino Cargar la solicitud de File Sync & Share.
- **URL de condiciones de la plataforma**. Esta página se abre cuando un administrador de socios hace clic en el enlace **Condiciones de la plataforma** en el panel **Acerca de** o en la pantalla de **Bienvenida** después del primer inicio de sesión.
- **URL de Declaración de privacidad**. Esta página se abre cuando un usuario hace clic en el enlace **Declaración de privacidad** en la pantalla de **Bienvenida** después del primer inicio de sesión, y en las páginas de destino Cargar la solicitud de File Sync & Share.

Importante
Si no desea que aparezca un documento en la pantalla de bienvenida, no introduzca la URL de ese documento.

Nota
Para obtener más información sobre Cargar las solicitudes de File Sync & Share, consulte el manual de usuario de Cyber Files Cloud.

Venta de productos de gama superior

- **URL de compra**. Esta página se abre cuando un usuario hace clic en **Comprar ahora** para actualizar su edición a una más avanzada del servicio Cyber Protection. Para obtener más información acerca de situaciones de venta de productos de gama superior, consulte "Configuración de situaciones relacionadas con la venta de productos de gama superior a sus clientes".

Aplicaciones para móviles

- **App Store**. Esta página se abre cuando el usuario hace clic en **Añadir** > **iOS** en el servicio **Cyber Protection** .
- **Google Play**. Esta página se abre cuando el usuario hace clic en **Añadir** > **Android** en el servicio **Cyber Protection** .

Configuración del servidor de correo electrónico

Puede especificar un servidor de correo electrónico personalizado que se utilizará para enviar notificaciones por correo electrónico desde el portal de gestión y los servicios. Para especificar un servidor de correo electrónico personalizado, haga clic en**Personalizar** y, a continuación, especifique los siguientes parámetros:

- En **De**, introduzca el nombre que aparecerá en el campo **De** en las notificaciones de correo electrónico.
- En el campo **SMTP**, escriba el nombre del servidor de correo saliente (SMTP).
- En **Puerto**, introduzca el puerto del servidor de correo saliente (SMTP). El puerto predeterminado es el 25.
- En **Cifrado**, seleccione si desea utilizar el cifrado TLS o SSL. Seleccione **Ninguno** para deshabilitar el cifrado.
- En **Nombre de usuario** y **Contraseña**, especifique las credenciales de una cuenta que se utilizará para enviar mensajes.

Configuración de personalización de marca

1. Inicie sesión en el portal de gestión.
2. Vaya hasta el inquilino en el que desee configurar la personalización de marca.
3. Haga clic en **Configuración** > **Personalización de marca**.
4. [Si aún no se ha habilitado la personalización de marca] Haga clic en **Habilitar personalización**

de marca.

5. Configure los elementos de personalización de marca anteriormente descritos.

Restaurar la configuración predeterminada de personalización de marca.

Puede restablecer todos los elementos de personalización de marca a sus valores predeterminados.

1. Inicie sesión en el portal de gestión.
2. Vaya hasta el inquilino en el que desee restablecer la personalización de marca.
3. Haga clic en **Configuración** > **Personalización de marca**.
4. Haga clic en **Restaurar valores predeterminados** en la esquina superior derecha.

Deshabilitar la personalización de marca

Puede deshabilitar la personalización de marca de su cuenta y de todos los inquilinos secundarios.

1. Inicie sesión en el portal de gestión.
2. Vaya hasta el inquilino en el que desee deshabilitar la personalización de marca.
3. Haga clic en **Configuración** > **Personalización de marca**.
4. Haga clic en **Deshabilitar personalización de marca** en la esquina superior derecha.

Marcas blancas

Puede controlar si el agente de Cyber Protection (para Windows, macOS y Linux) y el monitor de Cyber Protection (para Windows, macOS y Linux) tendrán o no marca para todos sus clientes y partners secundarios. Si habilita la marca blanca, el agente y Tray Monitor no tendrán marca. Esta configuración también afectará a los nombres y logotipos usados en el instalador y el monitor de Cyber Protection.

Aplicar etiquetas blancas

1. Inicie sesión en el portal de gestión.
2. Vaya hasta el inquilino en el que desee aplicar etiquetas blancas.
3. Haga clic en **Configuración** > **Personalización de marca**.
4. En la parte superior de la ventana, haga clic en **Etiqueta blanca** para borrar todos los elementos de personalización de marca, excepto **Nombre del servicio**, **URL del Acuerdo de licencia para el usuario final (EULA)**, **Manual del administrador del portal de gestión**, **Ayuda del administrador del portal de gestión**, y **Configuración del servidor de correo electrónico**.

Configuración de URL de la interfaz web personalizadas

Nota
Una URL personalizada apuntará a una dirección IP diferente en comparación con la URL predeterminada. Téngalo en cuenta a la hora de configurar las directivas de cortafuegos.

Pasos para configurar la URL de la interfaz web para los servicios de Cyber Protect Cloud

1. En el portal de administración, haga clic en **Configuración** > **Personalización de marca**.
2. En la sección **URL para los servicios de Cyber Protect Cloud**:
   - Haga clic en **Configurar** para establecer una URL personalizada por primera vez.
   - Haga clic en **Reconfigurar** para cambiar la URL personalizada existente.
3. En el paso **Configuración del dominio**, prepare su dominio y registro CNAME.
   Para utilizar una URL personalizada, debe tener un nombre de dominio activo y un registro CNAME configurado que apunte al centro de datos donde se encuentra la cuenta. La configuración del registro CNAME la realiza su registrador de DNS y puede tardar hasta 48 horas en propagarse.
   Para localizar el nombre de dominio de su centro de datos y solicitar la configuración de su registro CNAME, consulte el artículo URL de la consola web de marca (58275).
4. En el paso **Compruebe su URL**, verifique que la URL personalizada es accesible y que su registro CNAME se ha configurado correctamente. Para ello, introduzca el nombre de la URL principal y haga clic en **Comprobar**. Si utiliza un certificado SSL comodín, puede añadir hasta diez nombres de dominio alternativos. Si utiliza un certificado Let's Encrypt, se ignorarán los nombres de dominio alternativos.
5. En el paso **Certificado SSL**, puede llevar a cabo una de las siguientes acciones:
   - Crear un certificado Let's Encrypt. Para hacerlo, haga clic en **Certificado SSL gratis con Let's Encrypt**. Esta opción usa certificados "Let's Encrypt" emitidos por una entidad externa. El proveedor de servicios no se responsabiliza de los problemas derivados del uso de estos certificados gratuitos. Para obtener más información sobre los términos de Let's Encrypt, consulte https://letsencrypt.org/repository/.
   - Cargar un certificado comodín. Para hacerlo, haga clic en **Cargar certificado comodín** y proporcione un certificado comodín y una clave privada.
6. Haga clic en **Enviar** para aplicar los cambios.

Pasos para restablecer la URL personalizada a los valores predeterminados

1. En el portal de administración, haga clic en **Configuración** > **Personalización de marca**.
2. En la sección **URL para los servicios de Acronis Cyber Protect Cloud**, haga clic en **Restaurar a los valores predeterminados** para utilizar la URL predeterminada (https://cloud.acronis.com).

Actualización de agentes automáticamente

Cyber Protect tiene tres tipos de agentes que se pueden instalar en los equipos protegidos: Agente para Windows, Agente para Linux y Agente para Mac.

Cyber Files Cloud cuenta con una versión para Windows y otra para MacOS del agente de escritorio para File Sync & Share, que permite la sincronización de archivos y carpetas entre un equipo y el área de almacenamiento en la nube de File Sync & Share de un usuario para promover el trabajo offline, así como las prácticas de trabajo WFH (Trabaje desde casa) y BYOD (Traiga su propio dispositivo).

Para facilitar la gestión de varias cargas de trabajo, puede configurar (y deshabilitar) las actualizaciones automáticas y sin supervisión de todos los agentes en todos los equipos.

Importante
Actualmente, solo los partners y clientes con Protección habilitado tienen acceso a la funcionalidad de gestión de actualizaciones de agentes.

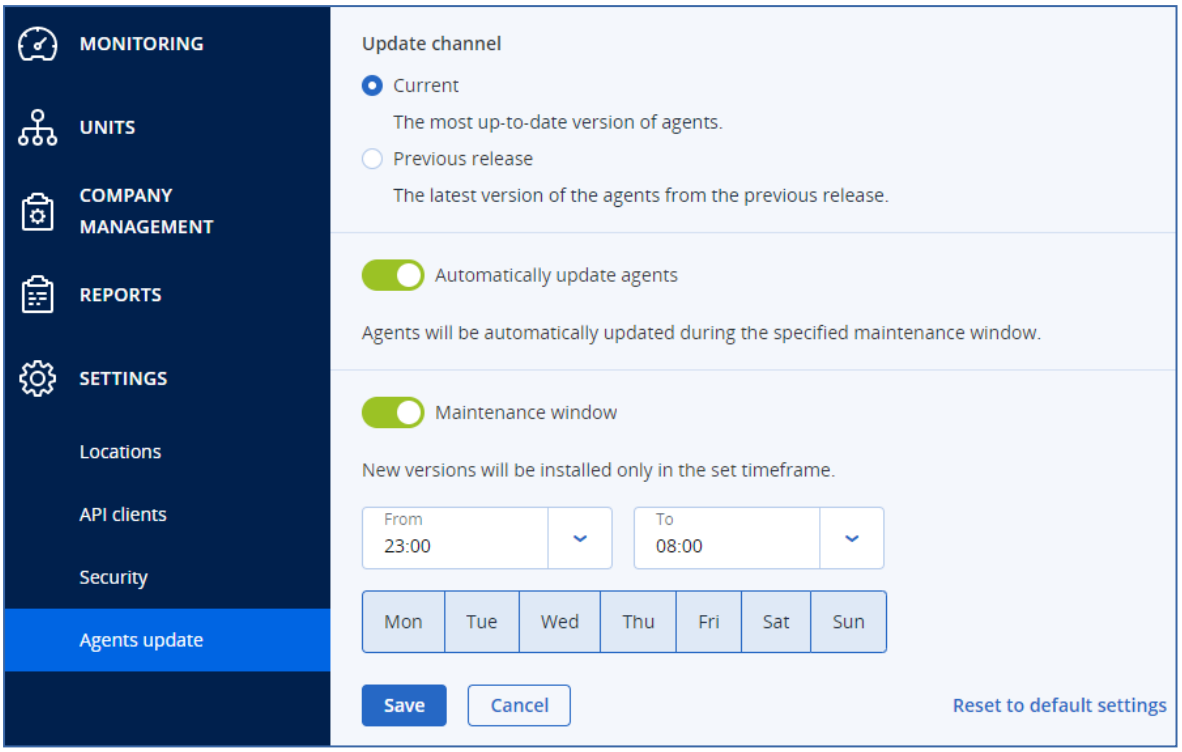
Nota
Para gestionar los agentes en equipos individuales y personalizar la configuración de las actualizaciones automáticas, consulte la actualización de agentes en la sección Manual del usuario de Cyber Protect.

Pasos para actualizar agentes automáticamente

Nota
Los partners y clientes que no tienen habilitada la protección heredan la configuración de la actualización automática del agente para File Sync & Share.

Pasos para establecer una actualización automática de los agentes desde la página inicial del portal de administración

1. Seleccione **Configuración > Actualización de agentes**.



2. Seleccione la versión que desea detectar para las actualizaciones automáticas: **Actual** o **Versión anterior**.
   (El valor predeterminado es **Actual**).
3. Active la **actualización automática de agentes**.
   (El valor predeterminado es **Activado**).
4. Establezca el margen de tiempo de mantenimiento.
   (El margen predeterminado es de 23:00 a 08:00).

   Nota
   Aunque los procesos de actualización de los agentes están diseñados para ser rápidos y fluidos, recomendamos elegir un margen de tiempo que provoque la mínima interrupción a los usuarios, ya que estos no pueden impedir o posponer las actualizaciones automáticas.

5. [Opcional] Seleccione días específicos para que se produzcan actualizaciones automáticas.
6. Seleccione **Guardar.**

Nota
Las actualizaciones automáticas solo están disponibles para:

- Agentes de Cyber Protect de la versión 15.0.26986 (publicada en mayo de 2021) o posterior.
- Agente de escritorio para File Sync & Share, versión 15.0.30370 o posterior.

Los agentes más antiguos se deben actualizar de forma manual a la versión más reciente antes de que se produzcan las actualizaciones automáticas.

Pasos para supervisar las actualizaciones de los agentes

Importante
Solo los administradores de los partners y clientes que tengan habilitado el módulo de protección pueden supervisar las actualizaciones de los agentes.

Para supervisar las actualizaciones de los agentes, consulte las secciones Alertas y Actividades del manual del usuario de Cyber Protect.

Supervisión

Para acceder a la información sobre las operaciones y el uso de los servicios, haga clic en **Supervisión**.

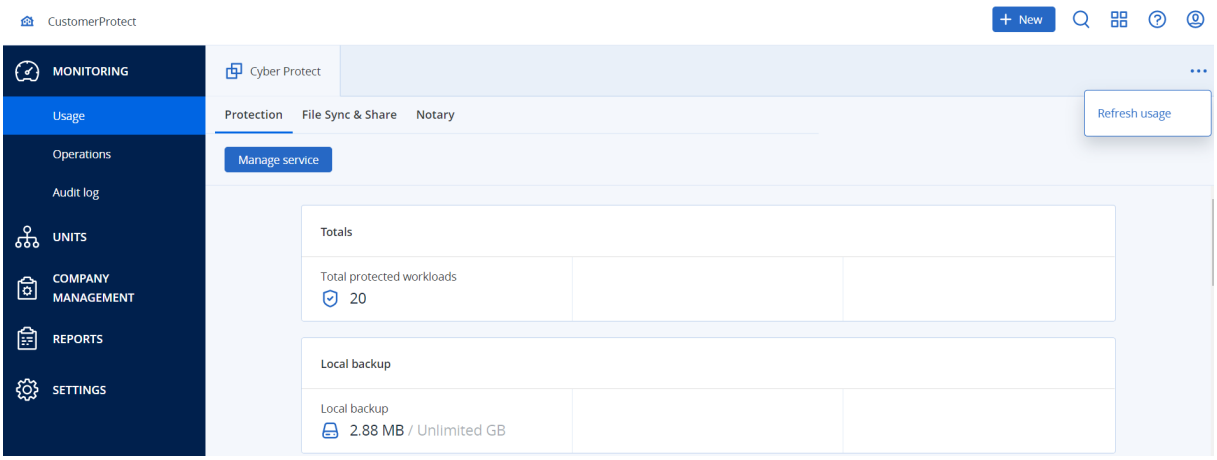
Uso

En la pestaña **Uso** se ofrece un resumen del uso del servicio y a través de ella se puede acceder a los servicios del inquilino en el que está operando.

El uso de datos incluye las características estándar y avanzadas.

Para actualizar los datos de uso que se muestran en la tabla, haga clic en la esquina superior derecha de la pantalla y seleccione **Actualizar uso**.

Nota
Puede llevar hasta 10 minutos recuperar los datos. Recargue la página para ver los datos actualizados.



Operaciones

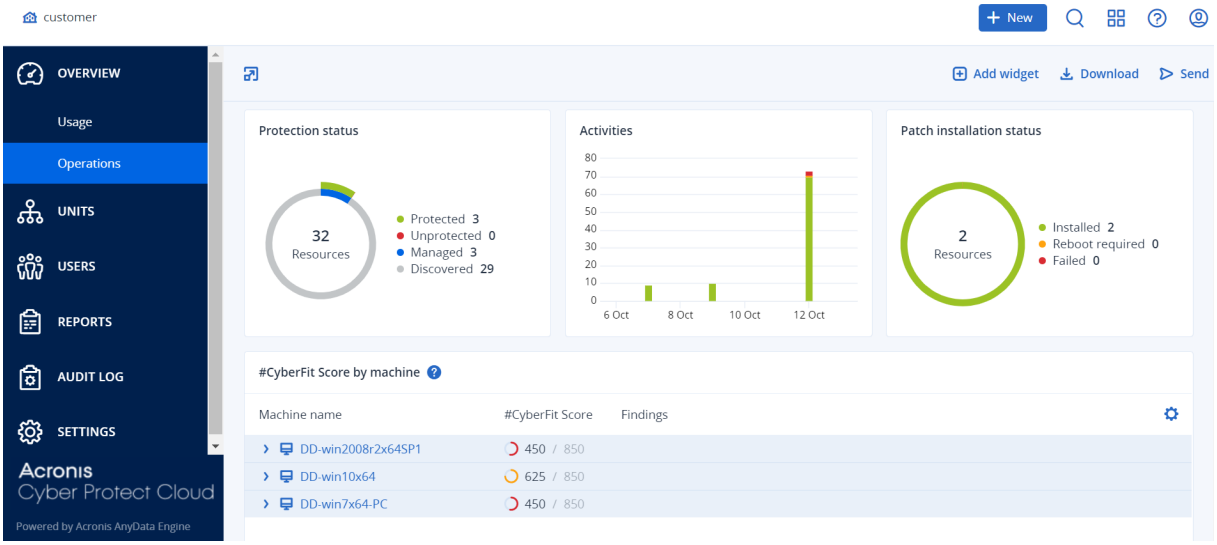
El panel de control **Operaciones** proporciona una serie de widgets personalizables que dan una imagen general de las operaciones relacionadas con el servicio de Cyber Protection. Los widgets de

otros servicios estarán disponibles en próximas versiones.

Los datos se muestran de forma predeterminada para el inquilino en el que está trabajando. Puede editar el inquilino que aparezca individualmente para cada widget para cambiarlo. También se muestra información adicional sobre los inquilinos cliente secundarios directos del inquilino seleccionado, incluidos los datos que se encuentran en carpetas. En el panel de información *no* se muestra información sobre los socios secundarios ni sus inquilinos; es usted quien debe profundizar en un socio en concreto para verlo en el panel de información. Sin embargo, si convierte un inquilino socio secundario en uno carpeta, la información sobre los clientes secundarios de este inquilino aparecerá en el panel de información del inquilino principal.

Los widgets se actualizan cada dos minutos. Los widgets tienen elementos interactivos que le permiten investigar y solucionar problemas. Puede descargar el estado actual del panel de información en formato .pdf o .xls o bien enviarlo por correo electrónico a cualquier dirección, incluidos los destinatarios externos.

Puede elegir entre una gran variedad de widgets, presentados como tablas, gráficos circulares, diagramas de barras, listas y estructuras de árbol. Puede agregar varios widgets del mismo tipo para distintos inquilinos con diferentes filtros.



Pasos para reorganizar los widgets en el panel de información

Haga clic en los nombres de los widgets para arrastrarlos y soltarlos.

Pasos para editar un widget

Haga clic en el icono de lápiz situado al lado del nombre del widget. Al editar un widget, puede cambiarle el nombre, modificar el periodo de tiempo, seleccionar el inquilino para el que se muestran los datos y establecer filtros.

Pasos para agregar un widget

Haga clic en **Añadir widget** y, luego, realice uno de los siguientes procedimientos:

- Haga clic en el widget que quiera añadir. El widget se añadirá con la configuración predeterminada.
- Para editar el widget antes de añadirlo, haga clic en el ícono de engranaje cuando el widget esté seleccionado. Después de editar el widget, haga clic en **Listo**.

Pasos para eliminar un widget

Haga clic en el signo de X situado al lado del nombre del widget.

Estado de la protección

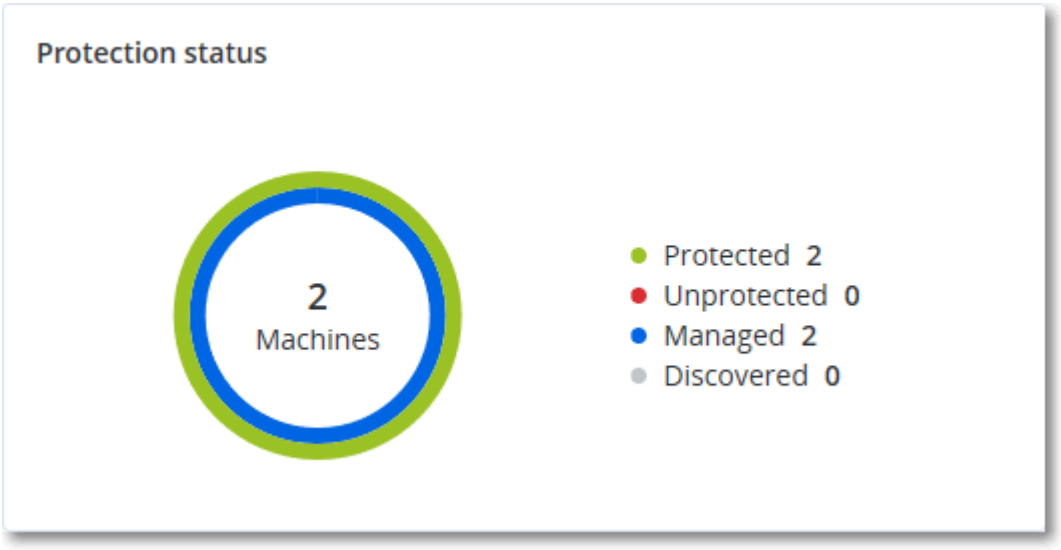
Estado de la protección

Este widget muestra el estado de protección actual de todos los equipos.

Un equipo puede encontrarse en uno de los siguientes estados:

- **Protegido**: equipos con un plan de protección aplicado.
- **Desprotegido**: equipos sin un plan de protección aplicado. Incluyen tanto a los equipos detectados como a los gestionados en los que no hay ningún plan de protección aplicado.
- **Gestionado**: equipos en los que está instalado un agente de protección.
- **Detectado**: equipos en los que no está instalado un agente de protección.

Si hace clic en el estado del equipo, se le redirigirá a la lista de equipos con este estado para que obtenga más información.



Equipos detectados

Este widget muestra la lista de equipos detectados en el intervalo de tiempo especificado.

Discovered machines

Device name	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

#CyberFit Score por equipo

Este widget muestra para cada equipo el #CyberFit Score total, las puntuaciones que lo componen e información sobre cada uno de los parámetros evaluados:

- Antimalware
- Copia de seguridad
- Cortafuegos
- VPN
- Cifrado
- Tráfico NTLM

Para mejorar la puntuación de cada parámetro, puede consultar las recomendaciones disponibles en el informe.

Para obtener más información sobre #CyberFit Score, consulte "#CyberFit Score para equipos".

#CyberFit Score by machine

Metric	#CyberFit Score	Findings
DESKTOP-2N2TRE8	625 / 850	
Anti-malware	275 / 275	You have anti-malware protection enabled
Backup	175 / 175	You have a backup solution protecting your data
Firewall	175 / 175	You have a firewall enabled for public and private networks
VPN	0 / 75	No VPN solution was found, your connection to public and shared networks is n...
Encryption	0 / 125	No disk encryption was found, your device is at risk from physical tampering
NTLM traffic	0 / 25	Outgoing NTLM traffic to remote servers is not denied, your credentials may be ...

Widgets de Detección y respuesta de endpoints (EDR)

Importante
Es una versión de Acceso Temprano de la documentación de EDR. Algunas de las funciones y descripciones pueden estar incompletas.

La Detección y respuesta de endpoints (EDR) incluye un número de widgets a los que se puede acceder desde el panel de control **Operaciones**.

Los widgets disponibles son los siguientes:

- Distribución de los principales incidentes por carga de trabajo
- Tiempo medio de reparación de incidentes
- Gráfico de quemado de incidentes de seguridad
- Estado de la red de las cargas de trabajo

Distribución de los principales incidentes por carga de trabajo

Este widget muestra las cinco cargas de trabajo con más incidentes (haga clic en **Mostrar todo** para volver a la lista de incidentes, que se filtra según los ajustes del widget).

Mantenga el ratón encima de la fila de una carga de trabajo para ver un desglose del estado actual de la investigación de los incidentes; los estados de la investigación son **No iniciada**, **Investigando**, **Cerrada** y **Falso positivo**. A continuación, haga clic en la carga de trabajo que desea analizar en profundidad y seleccione el cliente correspondiente en la notificación mostrada. La lista de incidentes se actualiza según los ajustes del widget.

Tiempo medio de reparación de incidentes

Este widget muestra el tiempo medio de reparación de incidentes de seguridad. Indica la rapidez con la que se investigan y reparan los incidentes.

Haga clic en una columna para ver un desglose de incidentes según la gravedad (**Crítica**, **Alta** y **Media**) y una indicación sobre cuánto tardan en repararse los distintos niveles de gravedad. El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.

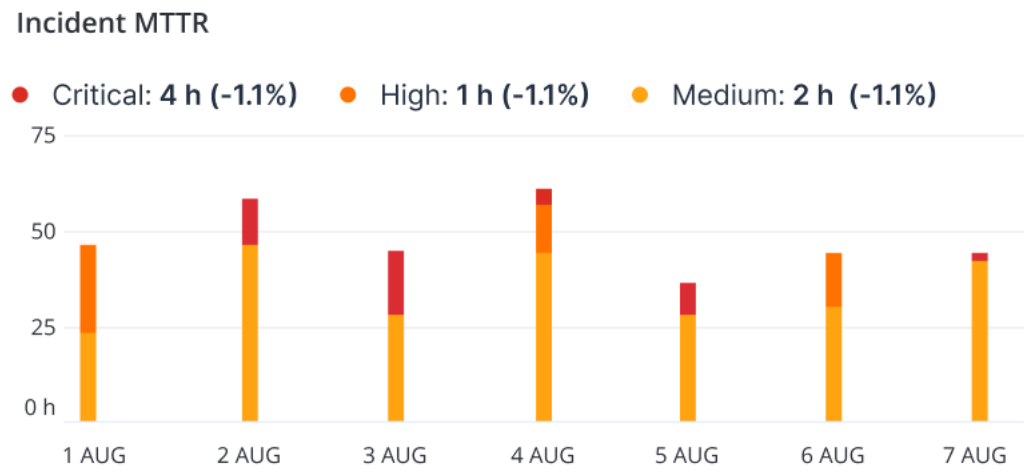
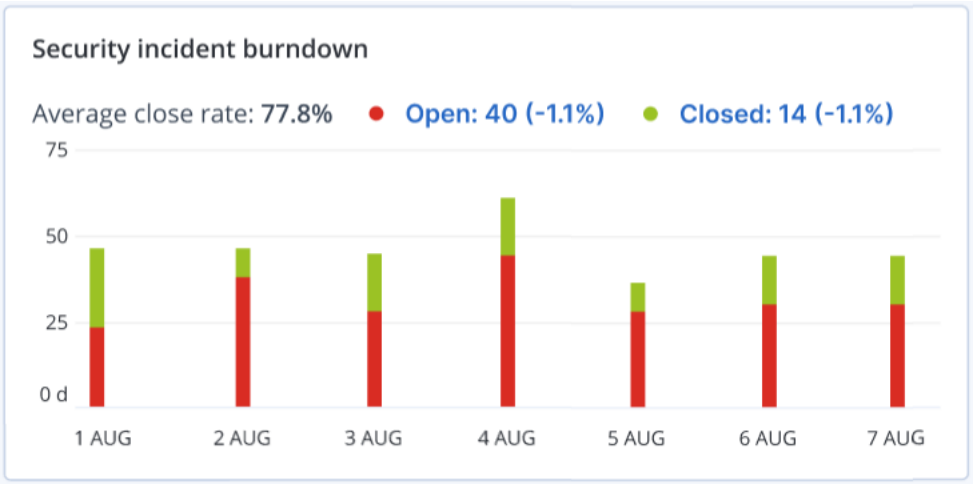


Gráfico de quemado de incidentes de seguridad

Este widget muestra la tasa de eficiencia de incidentes cerrados; el número de incidentes abiertos se mide comparado con el número de incidentes cerrados en un periodo de tiempo.

Mantenga el ratón encima de una columna para ver un desglose de los incidentes cerrados y abiertos del día seleccionado. Si hace clic en el valor Abierto, se muestra una ventana emergente para seleccionar el inquilino correspondiente. Aparece la lista de incidentes filtrados del inquilino seleccionado para mostrar los incidentes abiertos actualmente (en los estados **Investigando** o **No iniciada**). Si hace clic en el valor Cerrado, se muestra la lista de incidentes para el inquilino seleccionado filtrada para mostrar los incidentes que ya no están abiertos (en los estados **Cerrada** o **Falso positivo**).

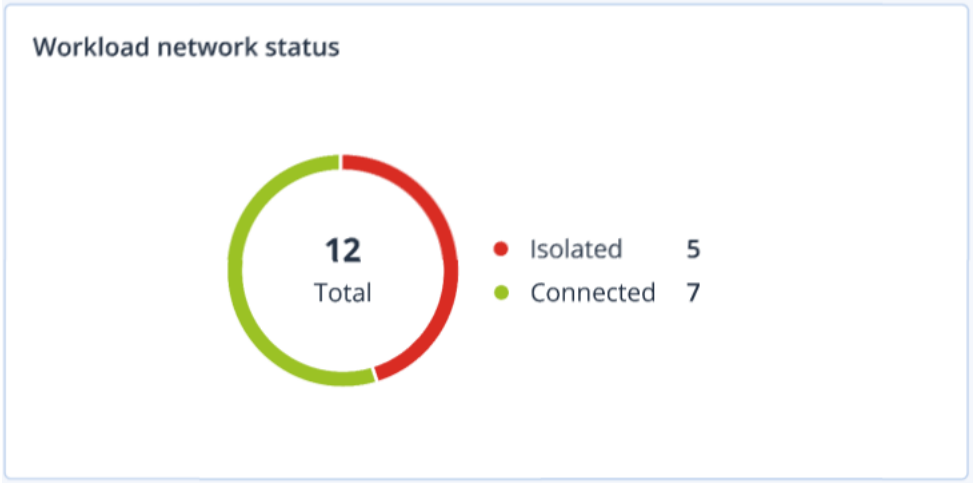
El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.



Estado de la red de las cargas de trabajo

Este widget muestra el estado de red actual de sus cargas de trabajo e indica cuántas están aisladas y cuántas conectadas.

Si hace clic en el valor Aislada, se muestra una ventana emergente para seleccionar el inquilino correspondiente. La vista de la carga de trabajo mostrada se filtra para que aparezcan las cargas de trabajo aisladas. Haga clic en el valor Conectada para ver la Carga de trabajo con la lista de agentes filtrada para mostrar las cargas de trabajo conectadas (para el inquilino seleccionado).



Supervisión del estado del disco

La supervisión del estado del disco proporciona información sobre el estado actual del disco y una previsión para que pueda evitar una pérdida de datos que pueda estar relacionada con un fallo del disco. Son compatibles tanto los discos duros como los SSD.

Limitaciones

- La previsión del estado del disco solo se puede realizar en equipos Windows.
- Únicamente se supervisan los discos de equipos físicos. Los discos de máquinas virtuales no se pueden supervisar ni aparecen en los widgets sobre el estado del disco.
- No se admiten configuraciones RAID.
- En unidades NVMe, solo es posible supervisar el estado del disco de las unidades que comunican los datos SMART mediante la API de Windows. La supervisión del estado del disco no es compatible con las unidades NVMe que necesitan leer los datos SMART directamente desde la unidad.

El estado del disco puede ser uno de los siguientes:

- **OK**:
  El estado del disco se encuentra entre el 70 y el 100 %.
- **Advertencia**:
  El estado del disco se encuentra entre el 30 y el 70 %.

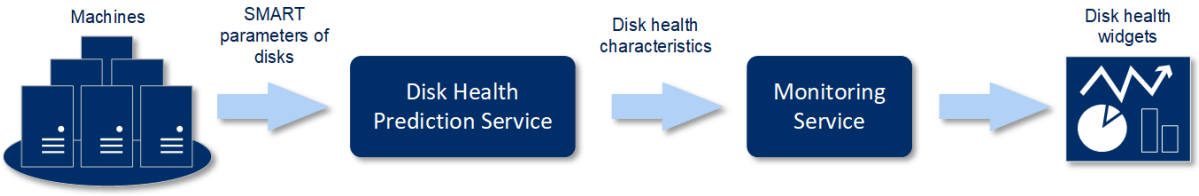
- **Crítico**:
  El estado del disco se encuentra entre el 0 y el 30 %.
- **Calculando datos del disco**:
  Se están calculando tanto el estado del disco actual como su previsión.

Cómo funciona

El servicio de predicción de estado del disco utiliza un modelo de predicción basado en la inteligencia artificial.

1. El agente de protección recopila los parámetros SMART de los discos y envía estos datos al servicio de predicción de estado del disco:
   - SMART 5: Número de sectores reasignados.
   - SMART 9: Horas durante las que está encendido.
   - SMART 187: Errores incorregibles de los que se ha informado.
   - SMART 188: Comando de tiempo de espera.
   - SMART 197: Número de sectores pendientes actuales.
   - SMART 198: Número de sectores incorregibles fuera de línea.
   - SMART 200: Tasa de error de escritura.
2. El servicio de previsión de estado de disco procesa los parámetros SMART recibidos, realiza predicciones y proporciona las siguientes características del estado del disco:
   - Estado actual del disco: OK, Advertencia, Crítico.
   - Previsión del estado del disco: negativa, estable, positiva.
   - Probabilidad de la previsión del estado del disco en porcentaje.

   El periodo de predicción es de un mes.
3. El servicio de supervisión recibe estas características y muestra la información relevante en los widgets del estado del disco en la consola de servicio.



Widgets sobre el estado del disco

Los resultados de la supervisión del estado del disco se muestran en los siguientes widgets que están disponibles en la consola de servicio.

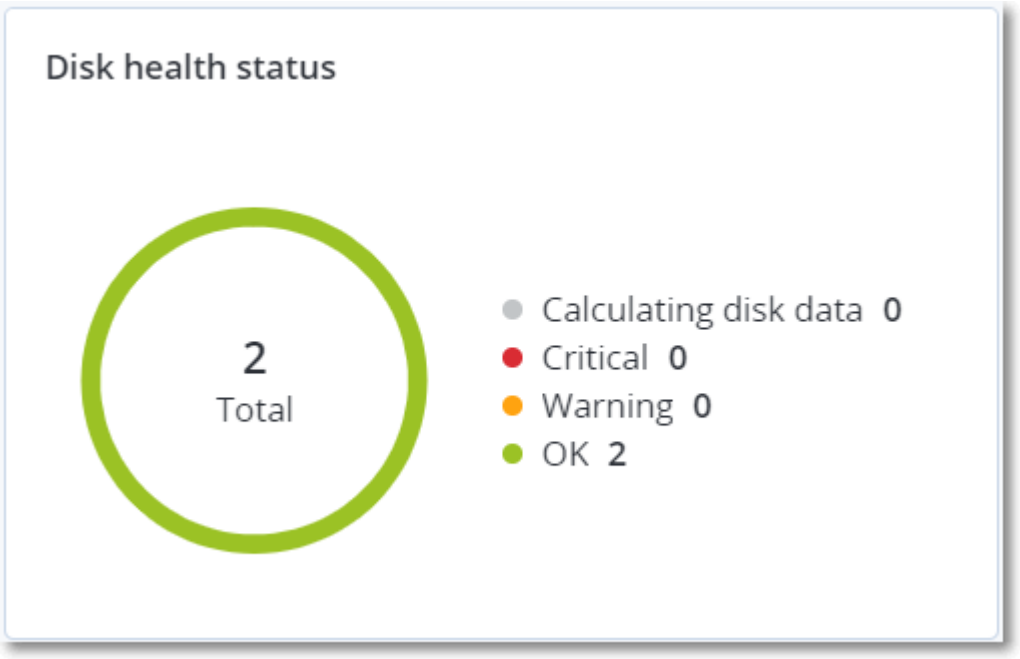
- **Resumen del estado del disco**: Es un widget en estructura de árbol con dos niveles de datos que se pueden cambiar al desplazarse.
  - Nivel de equipo:
    Muestra información resumida sobre el estado del disco de los equipos de los clientes

seleccionados. Solo se muestra el estado del disco más crítico. El resto de los estados aparecen en la información sobre herramientas cuando se pasa el ratón por encima de un bloque concreto. El tamaño del bloque del equipo depende del tamaño total de todos los discos del equipo. El color del bloque del equipo depende del estado del disco más crítico encontrado.

- Nivel de disco:
  Muestra el estado actual de todos los discos para el equipo seleccionado. Cada bloque de discos muestra el porcentaje de una de las siguientes previsiones del estado del disco y su probabilidad:
  - Se degradará
  - Permanecerá estable

- Mejorará

- **Estado del disco**: Es un widget con gráfico circular en el que se muestra el número de discos de cada estado.



Alertas sobre el estado del disco

La comprobación del estado del disco se ejecuta cada 30 minutos, pero la alerta correspondiente se genera una vez al día. Cuando el estado del disco cambia de **Advertencia** a **Crítico**, se genera siempre una alerta.

Nombre de la alerta	Gravedad	Estado del disco	Descripción
Es posible que falle el disco	Advertencia	(30 – 70)	Es probable que el disco <disk name> en este equipo falle en el futuro. Ejecute lo antes posible una copia de seguridad de imágenes completa de este disco, reemplácelo y, a continuación, recupere la imagen en el nuevo disco.
El fallo del disco es inminente	Crítico	(0 – 30)	El disco <disk name> en este equipo está en estado crítico y es bastante probable que falle muy pronto. En este punto, no se recomienda realizar una copia de seguridad de imágenes de este disco, ya que la carga añadida podría hacer que el disco falle. Realice inmediatamente una copia de seguridad de los archivos más importantes de este disco y reemplácelo.

Mapa de protección de datos

Gracias a la función del mapa de protección de datos, puede examinar todos los datos que sean importantes para usted y obtener información detallada sobre el número, el tamaño, la ubicación y el estado de protección de todos los archivos importantes en una vista escalable representada con una estructura de árbol.

El tamaño de cada bloque depende del tamaño o el número total de archivos importantes que pertenecen a un cliente o un equipo.

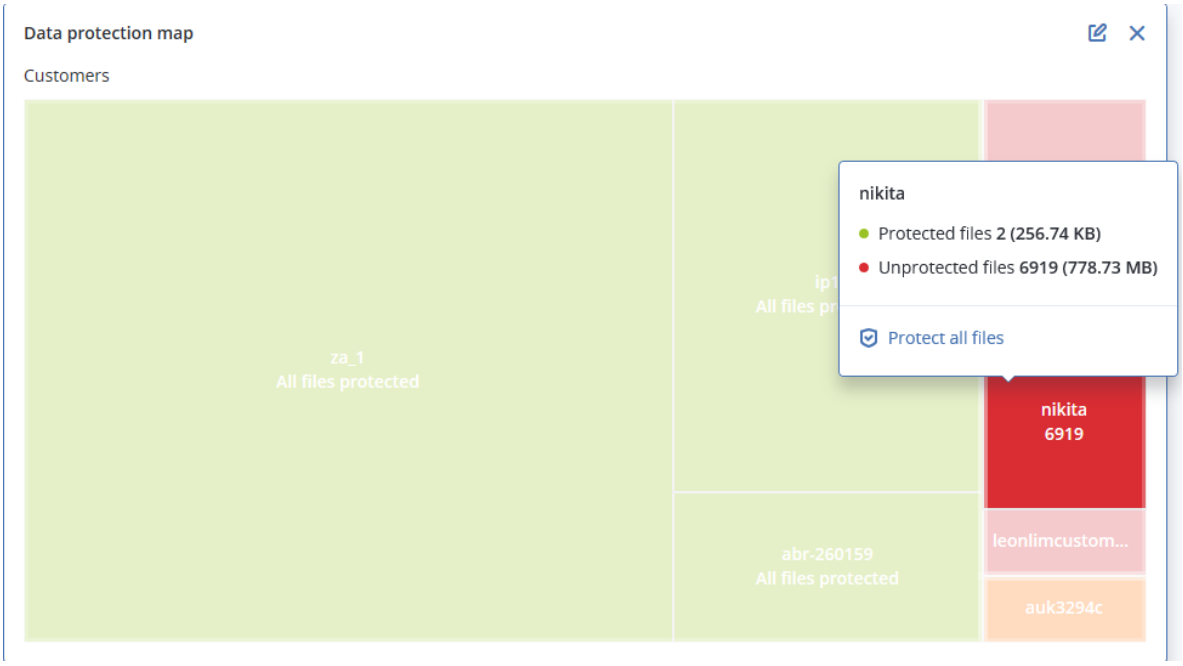
Los archivos pueden tener uno de los siguientes estados de protección:

- **Crítico**: hay entre un 51 y un 100 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ninguna copia de seguridad para la ubicación, el inquilino cliente o el equipo seleccionado.
- **Bajo**: hay entre un 21 y un 50 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ninguna copia de seguridad para la ubicación, el inquilino cliente o el equipo seleccionado.
- **Medio**: hay entre un 1 y un 20 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ninguna copia de seguridad para la ubicación, el inquilino cliente o el equipo seleccionado.

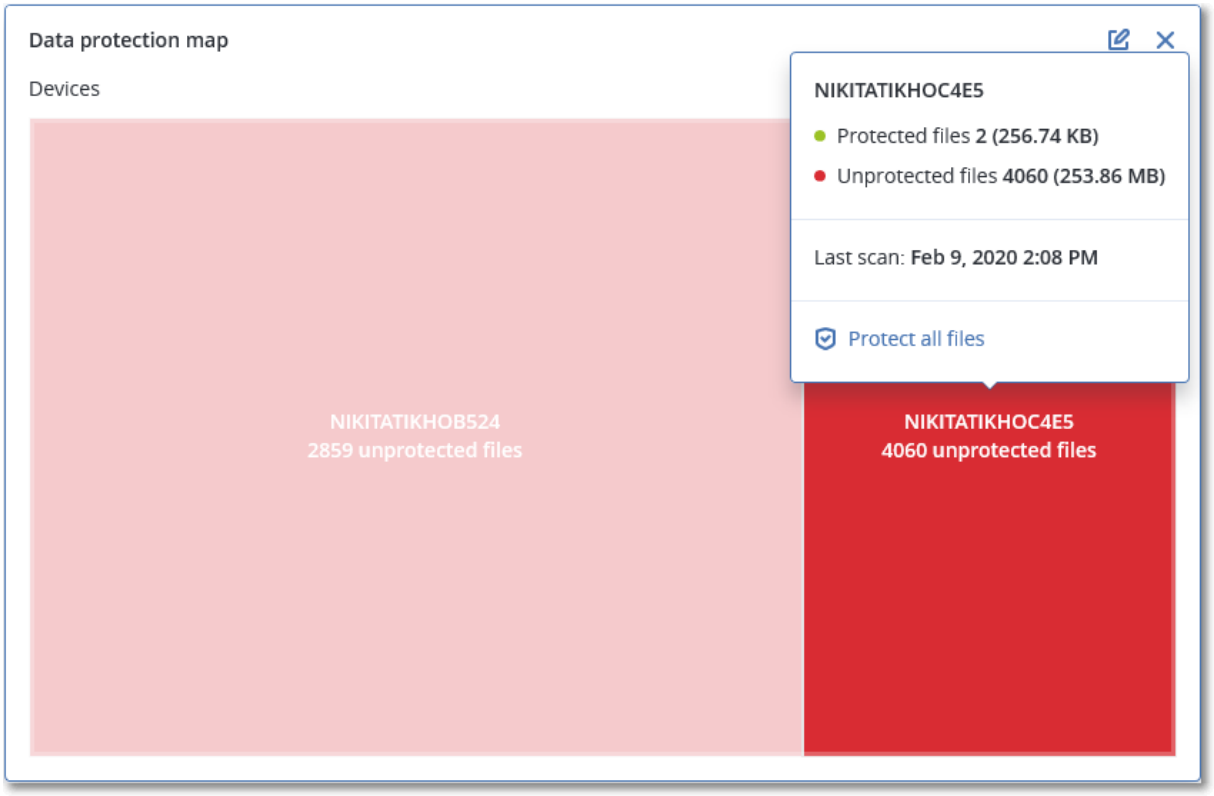
- **Alto**: todos los archivos con las extensiones que ha especificado están protegidos (se ha realizado una copia de seguridad de ellos) para la ubicación, el inquilino cliente o el equipo seleccionado.

Los resultados de la evaluación de la protección de datos se encuentran en el panel de control en el widget del mapa de protección de datos, un widget en estructura de árbol que tiene dos niveles de datos que se pueden cambiar al desplazarse:

- Nivel de inquilino cliente: muestra información resumida sobre el estado de protección de archivos importantes según los clientes que haya seleccionado.



- Nivel de equipo: muestra información sobre el estado de protección de archivos importantes según los equipos del cliente seleccionado.



Para proteger los archivos que no estén protegidos, pase el ratón por encima del bloque y haga clic en **Proteger todos los archivos**. En la ventana de diálogo encontrará información sobre el número de archivos que no están protegidos y su ubicación. Para protegerlos, haga clic en **Proteger todos los archivos**.

También puede descargar un informe detallado en formato CSV.

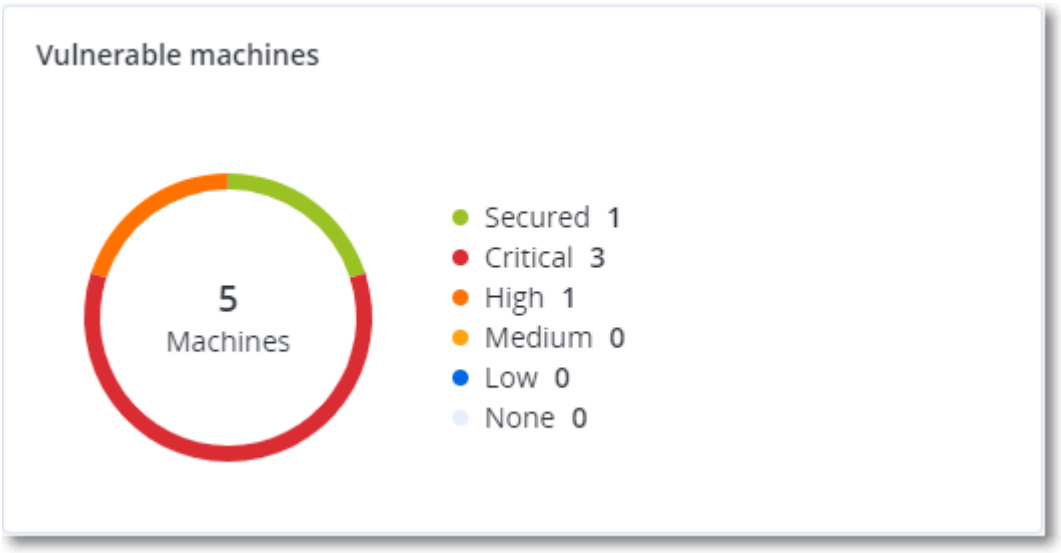
Widgets de evaluación de vulnerabilidades

Equipos vulnerables

Este widget muestra los equipos vulnerables por gravedad de la vulnerabilidad.

La vulnerabilidad encontrada tendrá uno de los siguientes niveles de gravedad de acuerdo con el sistema Common Vulnerability Scoring System (CVSS) v3.0:

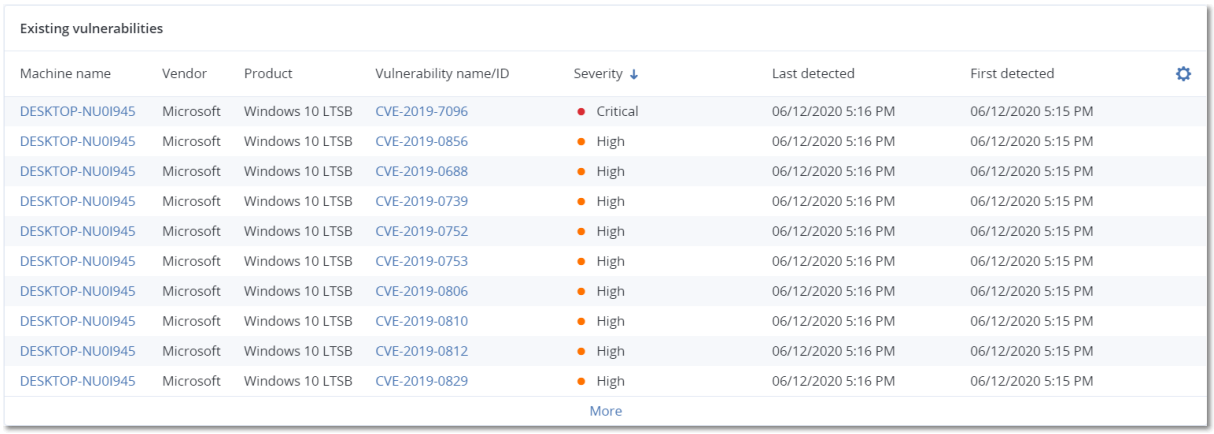
- Protegido: no se ha encontrado ninguna vulnerabilidad
- Crítico: 9,0-10,0 CVSS
- Alto: 7,0-8,9 CVSS
- Medio: 4,0-6,9 CVSS
- Bajo: 0,1-3,9 CVSS
- Ninguno: 0,0 CVSS



Vulnerabilidades existentes

Este widget muestra las vulnerabilidades que existen actualmente en los equipos. En el widget **Vulnerabilidades existentes**, hay dos columnas en las que se muestran determinadas marcas de hora y fecha:

- **Primera detección**: fecha y hora en que se detectó por primera vez una vulnerabilidad en el equipo.
- **Última detección**: fecha y hora en que se detectó por última vez una vulnerabilidad en el equipo.



Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

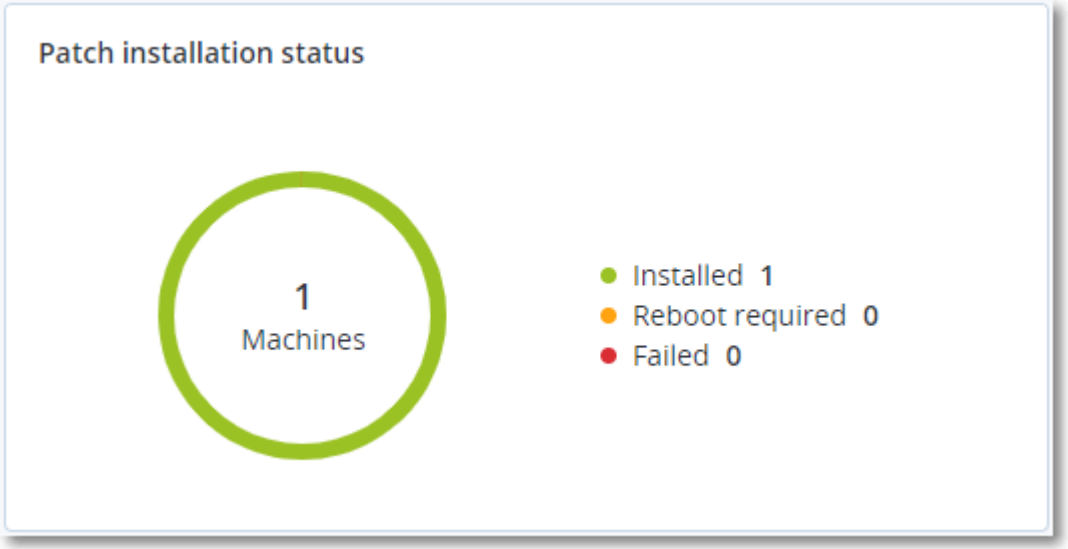
Widgets de instalación de parches

Hay cuatro widgets relacionados con la funcionalidad de gestión de parches.

Estado de instalación del parche

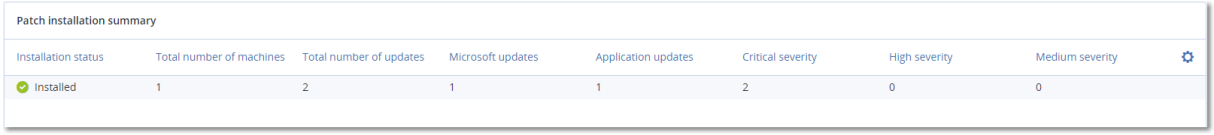
Este widget muestra el número de equipos agrupados por estado de instalación de parches.

- **Instalado**: todos los parches disponibles están instalados en el equipo.
- **Reinicio necesario**: después de la instalación de un parche, es necesario reiniciar el equipo.
- **Fallida**: la instalación del parche ha fallado en el equipo.



Resumen de la instalación del parche

Este widget muestra el resumen de parches que hay en los equipos por estado de instalación de parches.


Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

Historial de instalación de parches

Este widget muestra información detallada sobre los parches que hay en los equipos.

Patch installation history

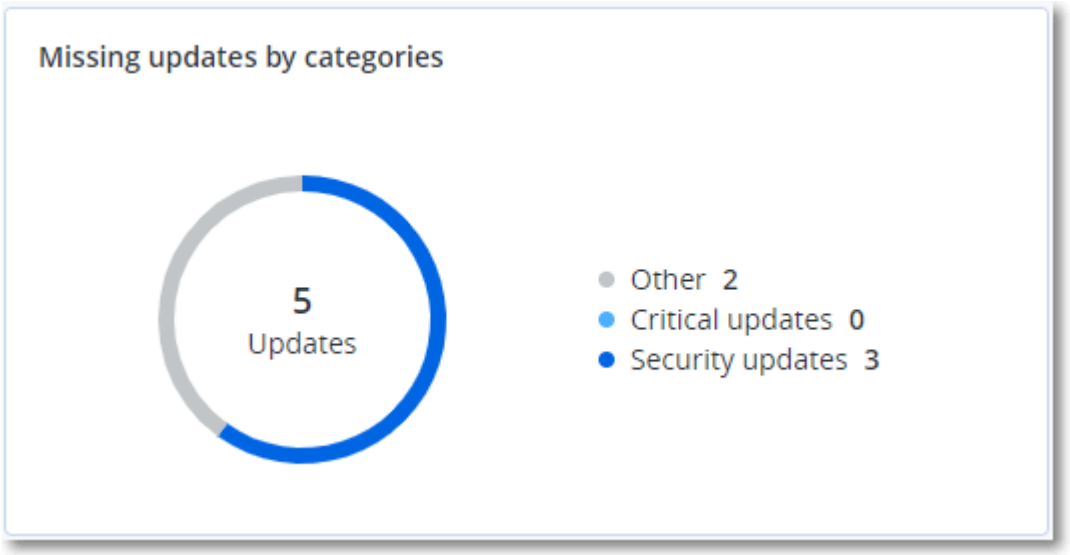
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020

More

Actualizaciones que faltan por categoría

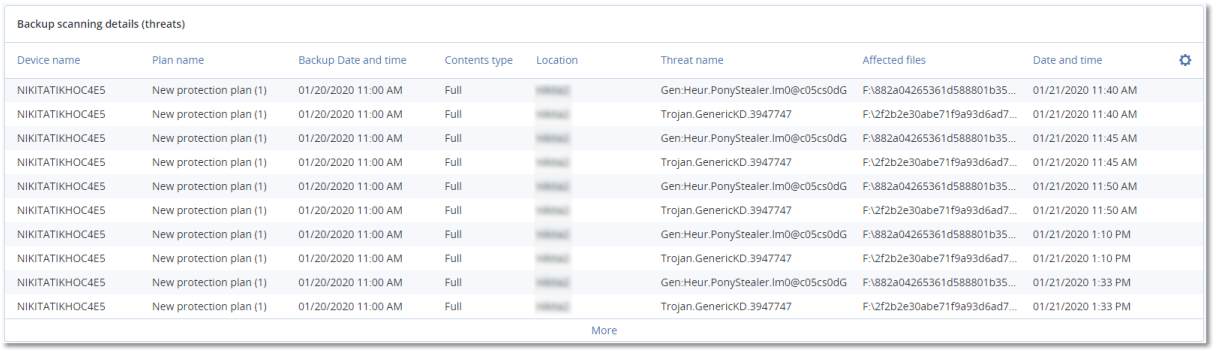
Este widget muestra el número de actualizaciones que faltan por categoría. Se muestran las siguientes categorías:

- Actualizaciones de seguridad
- Actualizaciones críticas
- Otros



Detalles del análisis de copias de seguridad

Este widget muestra información detallada sobre las amenazas detectadas en las copias de seguridad.

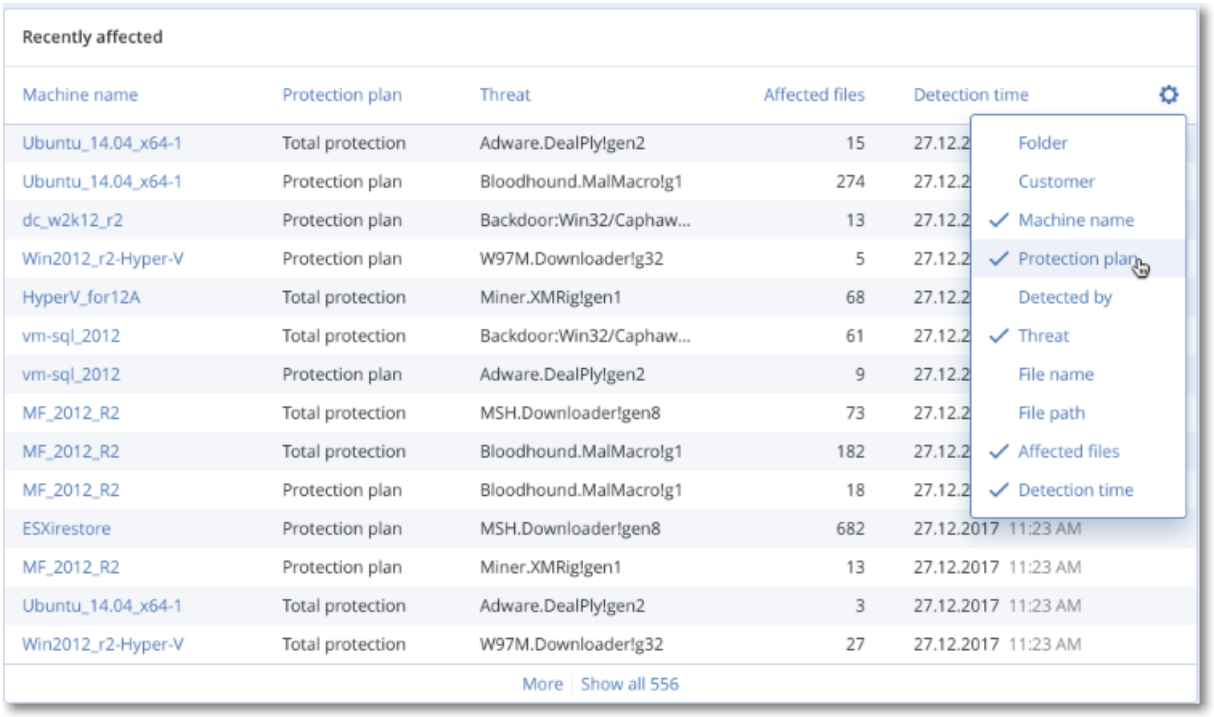

Backup scanning details (threats)

Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

Elementos afectados recientemente

Este widget muestra información detallada sobre las cargas de trabajo que se han visto afectadas por amenazas como virus, malware y ransomware. Puede encontrar información sobre las amenazas detectadas, la hora a la que se detectaron y el número de archivos que se vieron afectados.



Descargar datos de cargas de trabajo afectadas recientemente

Puede descargar los datos de las cargas de trabajo que se han visto afectadas, generar un archivo CSV y enviarlo a los destinatarios que especifique.

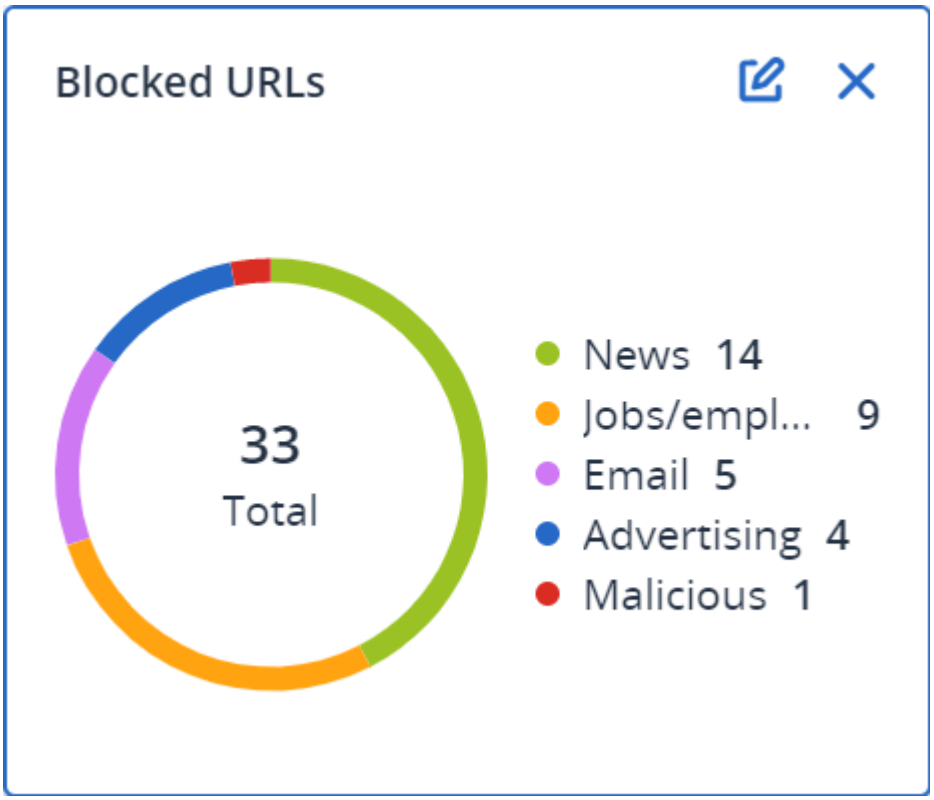
Para descargar los datos de las cargas de trabajo que se han visto afectadas, siga los siguientes pasos:

1. En el widget **Elementos afectados recientemente**, haga clic en **Descargar datos**.
2. En el campo **Período**, introduzca el número de días de los cuales desee descargar datos. Solo puede indicar 200 días como máximo.
3. En el campo **Destinatarios**, introduzca las direcciones de correo electrónico de todas las personas que recibirán un mensaje con un enlace para descargar el archivo CSV.
4. Haga clic en **Descargar**.

   El sistema empezará a generar el archivo CSV con los datos de las cargas de trabajo que se han visto afectadas en el período de tiempo que ha especificado. Cuando el archivo CSV se haya creado, el sistema enviará un correo electrónico a los destinatarios. Entonces, cada destinatario podrá descargar el archivo CSV.

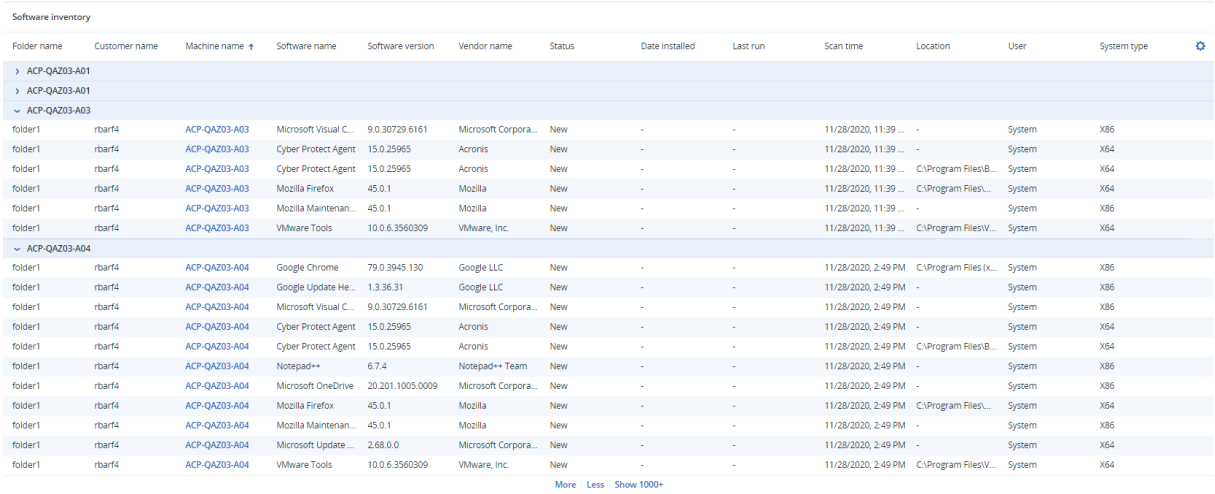
URL bloqueadas

El widget muestra las estadísticas de las URL bloqueadas por categoría. Para obtener más información acerca del filtrado y la categorización de las URL, consulte el manual del usuario de ciberprotección.



Widgets de inventario de software

El widget de tabla de **inventario de software** muestra información detallada sobre todo el software que se ha instalado en dispositivos de Windows y macOS en las organizaciones de sus clientes.

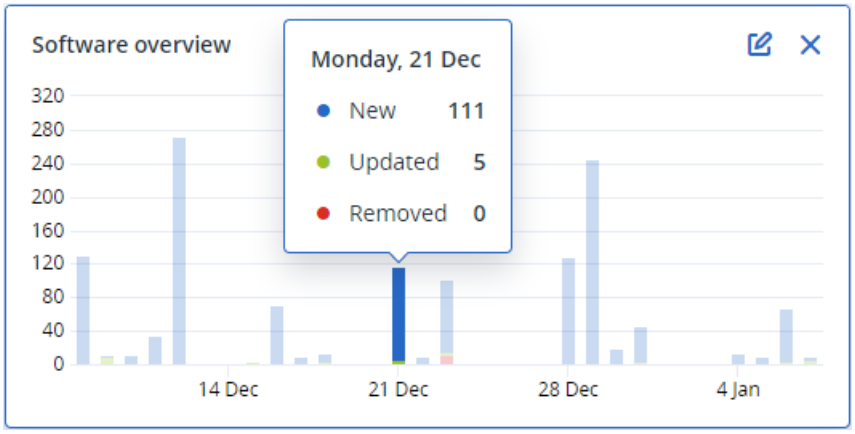


Software inventory

Folder name	Customer name	Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User	System type
ACP-QAZ03-A01												
ACP-QAZ03-A01												
ACP-QAZ03-A03												
folder1	rbarf4	ACP-QAZ03-A03	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	-	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\V...	System	X64
ACP-QAZ03-A04												
folder1	rbarf4	ACP-QAZ03-A04	Google Chrome	79.0.3945.130	Google LLC	New	-	-	11/28/2020, 2:49 PM	C:\Program Files (x...	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Google Update He...	1.3.36.31	Google LLC	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Notepad++	6.7.4	Notepad++ Team	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft OneDrive	20.201.1005.0009	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Update ...	2.68.0.0	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\V...	System	X64

More | Less | Show 1000+

El widget de **información general del software** muestra el número de aplicaciones nuevas, actualizadas y eliminadas en dispositivos de Windows y macOS en las organizaciones de sus clientes durante un período específico de tiempo (7 días, 30 días o el mes en curso).



Cuando pase el ratón sobre determinada barra del gráfico, aparecerá la siguiente información sobre la herramienta:

Nuevas: el número de aplicaciones instaladas recientemente.

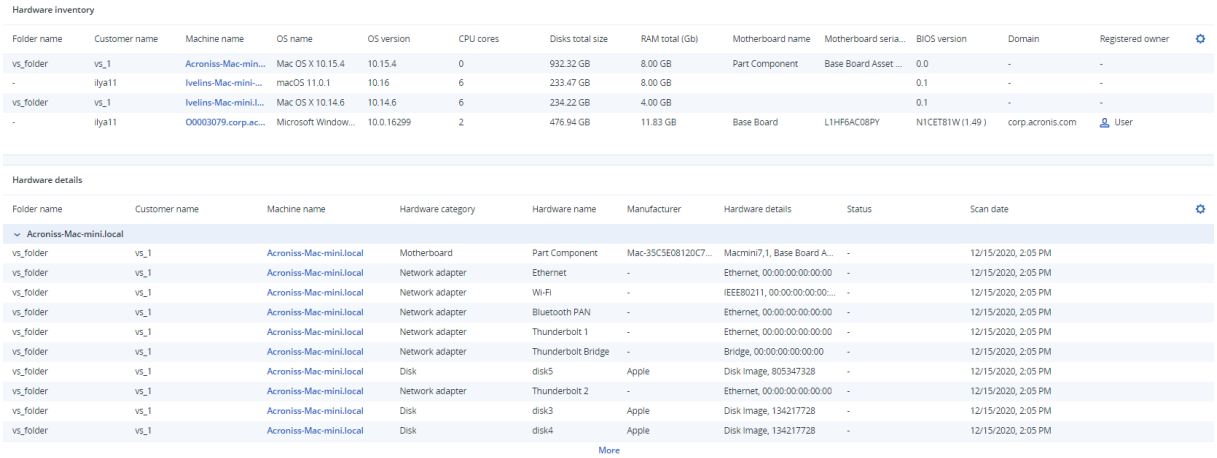
Actualizadas: el número de aplicaciones actualizadas.

Eliminadas: el número de aplicaciones eliminadas.

Cuando haga clic en la parte de la barra que corresponde a determinado estado, se cargará una ventana emergente. En ella se incluyen todos los clientes que tienen dispositivos con aplicaciones en el estado seleccionado y en las fechas seleccionadas. Al seleccionar un cliente de la lista, haga clic en **Ir al cliente** y se le redirigirá a la página **Gestión del software** -> **Inventario de software** en la consola de servicio de atención al cliente. La información que aparece en esa página está filtrada de acuerdo con la fecha y el estado correspondientes.

Widgets de inventario de hardware

Los widgets de tablas de **inventario de hardware** y de **detalles de hardware** muestran información sobre todo el hardware instalado en dispositivos físicos y virtuales de Windows y macOS en las organizaciones de sus clientes.


Hardware inventory

Folder name	Customer name	Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner
vs_folder	vs_1	Acroniss-Mac-min...	Mac OS X 10.15.4	10.15.4	0	932.32 GB	8.00 GB	Part Component	Base Board Asset ...	0.0	-	-
-	ilya11	Ivelins-Mac-mini-...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-
vs_folder	vs_1	Ivelins-Mac-mini.l...	Mac OS X 10.14.6	10.14.6	6	234.22 GB	4.00 GB			0.1	-	-
-	ilya11	O0003079.corp.ac...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User

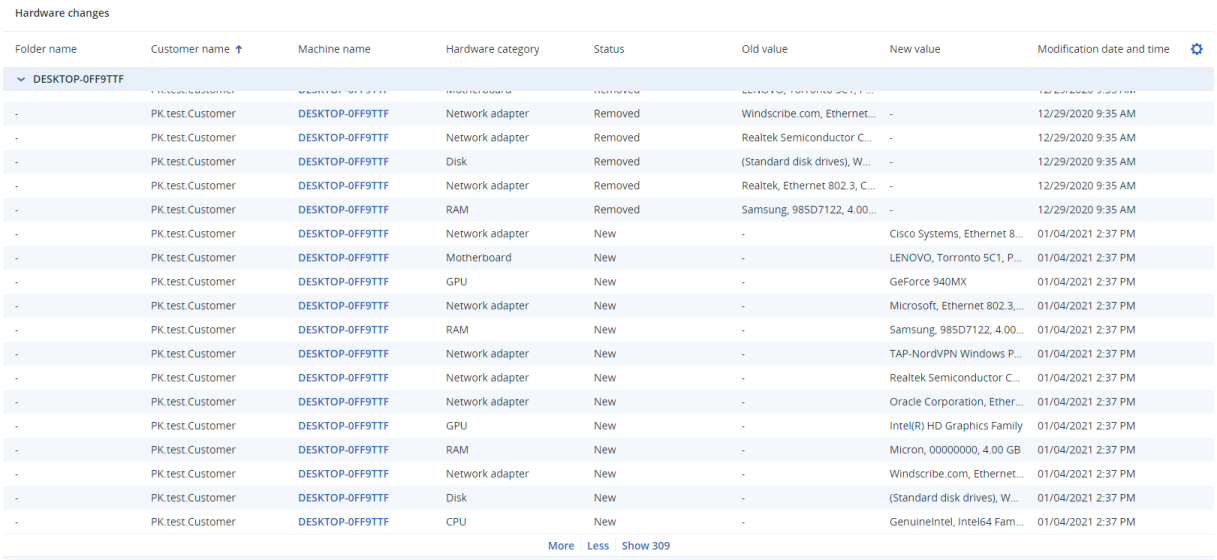
Hardware details

Folder name	Customer name	Machine name	Hardware category	Hardware name	Manufacturer	Hardware details	Status	Scan date
Acroniss-Mac-mini.local								
vs_folder	vs_1	Acroniss-Mac-mini.local	Motherboard	Part Component	Mac-35C5E08120C7...	Macmini7,1, Base Board A...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Ethernet	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Wi-Fi	-	IEEE80211, 00:00:00:00:00:...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Bluetooth PAN	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 1	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt Bridge	-	Bridge, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk5	Apple	Disk Image, 805347328	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 2	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk3	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk4	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM

More

El widget de tabla de **cambios de hardware** muestra información sobre el hardware que se ha añadido, eliminado y cambiado en dispositivos físicos y virtuales de Windows y macOS en las

organizaciones de sus clientes durante un período específico de tiempo (7 días, 30 días o el mes en curso).



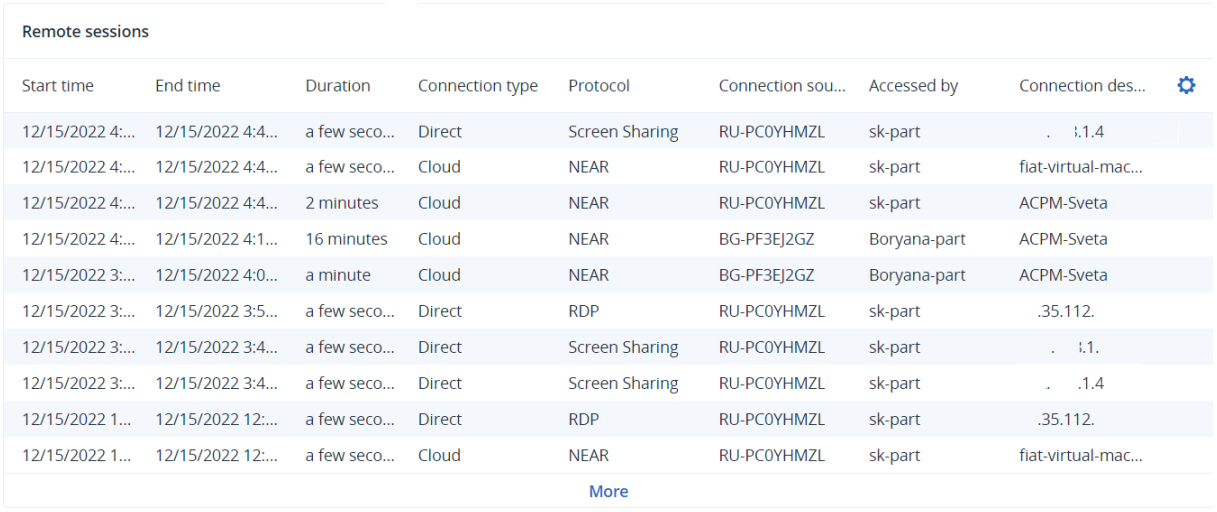
Hardware changes

Folder name	Customer name	Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF							
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Windscribe.com, Ethernet...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek Semiconductor C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	Removed	(Standard disk drives), W...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek, Ethernet 802.3, C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	Removed	Samsung, 985D7122, 4.00...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 8...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	GeForce 940MX	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Microsoft, Ethernet 802.3,...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor C...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ether...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Windscribe.com, Ethernet...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), W...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	CPU	New	-	GenuineIntel, Intel64 Fam...	01/04/2021 2:37 PM

More | Less | Show 309

Historial de sesión

El widget muestra la información detallada sobre las sesiones de escritorio remoto y de transferencia de archivos realizadas en las organizaciones de sus clientes durante un período de tiempo determinado.



Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

Generación de informes

Para crear informes sobre las operaciones y el uso de los servicios, haga clic en **Informes**.

Uso

Los informes de uso proporcionan datos históricos sobre la utilización de los servicios. Los informes de uso están disponibles en formato CSV y HTML.

Tipo de informe

Puede seleccionar uno de los siguientes tipos de informe:

- **Uso actual**

  En el informe se incluyen los parámetros de uso del servicio actuales.

  Las métricas de uso se calculan dentro de cada uno de los períodos de facturación de los inquilinos secundarios. Si los inquilinos incluidos en el informe tienen períodos de facturación distintos, el uso del inquilino primario puede ser diferente de la suma de los usos de los inquilinos secundarios.
- **Distribución de uso actual**

  Este informe solo está disponible para inquilinos socio gestionados a través de un sistema de aprovisionamiento externo. Este informe es útil cuando los periodos de facturación de los inquilinos secundarios no coinciden con los de los primarios. En el informe se incluyen los parámetros de uso del servicio de inquilinos secundarios calculados en el periodo de facturación actual del inquilino primario. Se garantiza que el uso del inquilino primario es igual a la suma de los usos de todos los inquilinos secundarios.
- **Resumen del período**

  En el informe se incluyen los parámetros de uso del servicio para el final del periodo especificado y la diferencia entre los parámetros del comienzo y el final del periodo especificado.
- **Día a día del período**

  En el informe se incluyen los parámetros de uso del servicio y sus cambios para cada día del periodo especificado.

Ámbito del informe

Puede seleccionar el ámbito del informe entre los valores siguientes:

- **Clientes y socios directos**

  El informe solo incluye las métricas de uso del servicio para los inquilinos secundarios inmediatos del inquilino en el que está operando.
- **Todos los socios y clientes**

  El informe incluirá las métricas de uso del servicio para todos los inquilinos secundarios del inquilino en el que está operando.
- **Todos los clientes y partners (incluyendo los detalles de usuario)**

  El informe incluirá las métricas de uso del servicio para todos los inquilinos secundarios del inquilino en el que está operando y para todos los usuarios dentro de los inquilinos.

Parámetros con uso cero

Puede reducir el número de filas en el informe si muestra la información sobre los parámetros cuyo uso sea distinto a cero y oculta la información de aquellos cuyo uso sea cero.

Configuración de los informes de uso planificados

Un informe programado recoge los parámetros de uso del servicio durante el último mes natural completo. Los informes se generan a las 23:59:59 (hora UTC) del primer día del mes y se envían el segundo día. Los informes se envían a todos los inquilinos que tengan marcada la casilla de verificación **Informes de uso planificados** seleccionada en la configuración del usuario.

Para habilitar o deshabilitar un informe programado

1. Inicie sesión en el portal de gestión.
2. Asegúrese de que opera en el máximo inquilino disponible para usted.
3. Haga clic en **Informes** > **Uso**.
4. Haga clic en **Programado**.
5. Seleccione o deseleccione la casilla de verificación de informes **Enviar un resumen mensual**
6. En **Nivel de detalle**, seleccione el ámbito del informe.
7. [Opcional] Seleccione **Ocultar parámetros con uso cero** si no desea incluir parámetros con uso cero en el informe.

Configuración de los informes de uso personalizados

Este tipo de informe no puede planificarse, se genera a petición. El informe se enviará a su dirección de correo electrónico.

Para generar un informe personalizado

1. Inicie sesión en el portal de gestión.
2. Vaya hasta el inquilino para el que desea crear un informe.
3. Haga clic en **Informes** > **Uso**.
4. Seleccione la pestaña **Personalizado**.
5. En **Tipo**, seleccione el tipo de informe como se ha descrito anteriormente.
6. [No disponible para el tipo de informe **Uso actual**] En **Período**, seleccione el período del informe:
   - **Mes actual**
   - **Mes anterior**
   - **Personalizado**
7. [No disponible para el tipo de informe **Uso actual**] Si quiere especificar un período de informe personalizado, seleccione las fechas de inicio y fin. De lo contrario, omita este paso.
8. En **Nivel de detalle**, seleccione el ámbito del informe, como se ha descrito anteriormente.
9. [Opcional] Seleccione **Ocultar parámetros con uso cero** si no desea incluir parámetros con uso cero en el informe.
10. Para generar el informe, haga clic en **Generar y enviar**.

Informes de operaciones

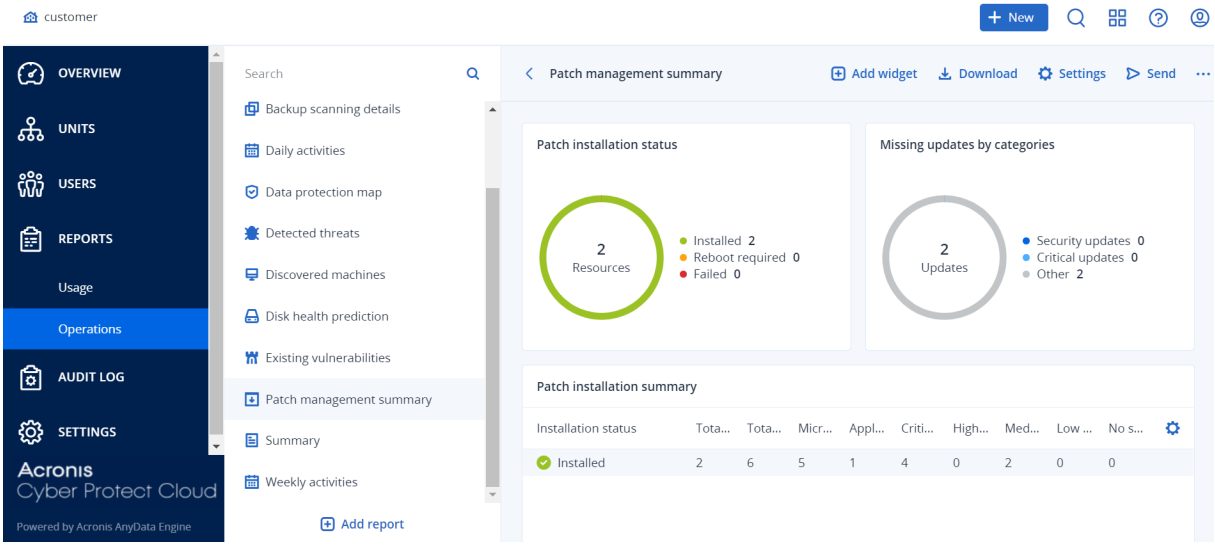
Un informe sobre operaciones puede incluir cualquier conjunto de los widgets del panel de información **Operaciones**. De forma predeterminada, todos los widgets muestran la información de resumen del inquilino en el que está trabajando. Puede editar esto individualmente para cada widget para cambiarlo o para todos los widgets en la configuración del informe.

Según el tipo de widget, el informe incluye datos para un intervalo de tiempo o para el momento de la navegación o generación de informes. Consulte "Datos informados según el tipo de widget" (p. 124).

Todos los widgets históricos muestran la información del mismo intervalo de tiempo. Puede cambiar este intervalo en la configuración de los informes.

Puede utilizar informes predeterminados o crear uno personalizado.

Puede descargar un informe sobre operaciones o enviarlo por correo electrónico en formato Excel (XLSX) o PDF.



Los informes predeterminados se indican a continuación:

Nombre del informe	Descripción
#CyberFit Score por equipo	Muestra el #CyberFit Score, basado en la evaluación de parámetros de seguridad y en la configuración de cada equipo, así como las recomendaciones para mejoras.
Alertas	Muestra las alertas que se producen durante un periodo especificado.
Detalles del análisis de copias de seguridad	Muestra información detallada sobre las amenazas detectadas en las copias de seguridad.
Actividades diarias	Muestra información resumida sobre las actividades realizadas

	durante un periodo especificado.
Mapa de protección de datos	Muestra información detallada sobre el número, el tamaño, la ubicación y el estado de protección de todos los archivos importantes de los equipos.
Amenazas detectadas	Muestra información sobre los equipos afectados por número de amenazas bloqueadas, así como la de los equipos en buen estado y los vulnerables.
Equipos detectados	Enumera todos los equipos hallados en la red de la organización.
Predicción del estado del disco	Muestra predicciones de cuándo se deteriorará el disco duro/SSD y del estado actual del disco.
Vulnerabilidades existentes	Muestra las vulnerabilidades existentes en el sistema operativo de su organización. El informe también muestra información de los equipos afectados en su red respecto a cada producto enumerado.
Resumen de gestión de parches	Muestra el número de parches que faltan, los instalados y los aplicables. Puede desglosar los informes para obtener información sobre los parches que faltan y los instalados, así como detalles de todos los sistemas.
Resumen	Muestra la información resumida sobre los dispositivos protegidos durante un periodo especificado.
Actividades semanales	Muestra información resumida sobre las actividades realizadas durante un periodo especificado.
Inventario de software	Muestra información detallada sobre todo el software instalado en equipos de Windows y macOS en las organizaciones de sus clientes.
Inventario de hardware	Muestra información detallada sobre todo el hardware disponible en equipos físicos y virtuales de Windows y macOS en las organizaciones de sus clientes.
Sesiones remotas	Muestra la información detallada sobre las sesiones de escritorio remoto y de transferencia de archivos realizadas en las organizaciones de sus clientes durante un período de tiempo determinado.

Para ver un informe, haga clic en su nombre.

Para acceder a las operaciones que cuenten con un informe, haga clic en el icono de puntos suspensivos verticales de la línea de informes. Desde dentro del informe están disponibles las mismas operaciones.

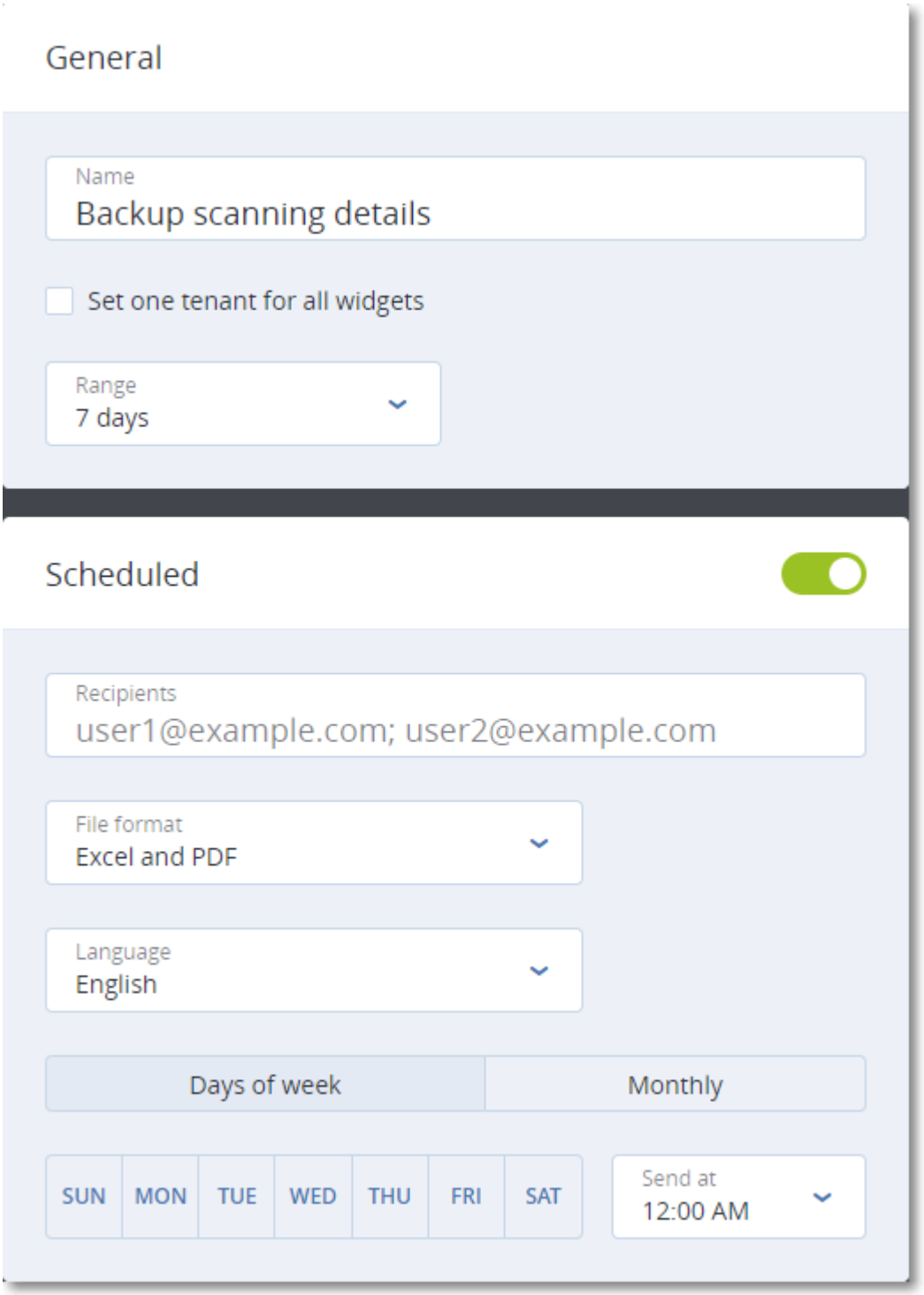
Incorporación de un informe

1. Haga clic en **Añadir informe**.
2. Realice uno de los siguientes procedimientos:
   - Para añadir un informe predefinido, haga clic en su nombre.
   - Para añadir un informe personalizado, haga clic en **Personalizado** y en el nombre del informe (el nombre asignado de forma predeterminada será similar a "**Personalizado(1)**") y, a continuación, añada widgets al informe.
3. [Opcional] Arrastre y suelte los widgets para reorganizarlos.
4. [Opcional] Edite el informe tal y como se describe a continuación.

Edición de la configuración de informes

Para editar un informe, haga clic en su nombre y, luego, en **Configuración**. Al editar un informe puede llevar a cabo las siguientes acciones:

- Cambiarle el nombre
- Cambiar el inquilino que se muestra para todos los widgets incluidos en él
  Si tiene inquilinos secundarios, dispone de la opción **Establecer un inquilino para todos los widgets**. Esta opción permite filtrar los datos de todos los widgets del informe por el inquilino seleccionado. Si la opción no está seleccionada, los widgets mostrarán datos de todos los inquilinos secundarios de su inquilino actual.
- Cambiar el intervalo de tiempo de todos los widgets incluidos en él
- Planificar su envío por correo electrónico en formato PDF o Excel.



Programación de un informe

1. Haga clic en el nombre del informe y, luego, en **Configuración**.
2. Habilite el conmutador **Planificado**.
3. Especifique la dirección de correo electrónico de los destinatarios.
4. Seleccione el formato del informe: PDF, Excel o ambos.

5. Seleccione los días y la hora en que se enviará el informe.
6. Haga clic en **Guardar** en la esquina superior derecha.

Exportación e importación de la estructura del informe

Puede exportar e importar la estructura del informe (el conjunto de widgets y su configuración) a un archivo JSON. Esto puede ser útil para copiar la estructura del informe de un inquilino en otro.

Para exportar la estructura del informe, haga clic en el nombre del informe, en el icono de puntos suspensivos vertical de la esquina superior derecha y, a continuación, en **Exportar**.

Para importar la estructura del informe, haga clic en **Añadir informe** y, a continuación, en **Importar**.

Descargar un informe

Puede descargar un informe. Para ello, haga clic en **Descargar** y seleccione los formatos que necesite:

- Excel y PDF
- Excel
- PDF

Volcado de los datos del informe

Puede enviar un volcado de los datos del informe en un archivo CSV por correo electrónico. El volcado incluye todos los datos del informe (sin filtrado) para un intervalo de tiempo personalizado. Las marcas de hora y fecha de los informes CSV están en formato UTC, mientras que en los informes en Excel y PDF las marcas de hora y fecha están en la zona horaria del sistema actual.

El software genera el volcado de datos sobre la marcha. Si especifica un periodo largo, esta acción puede tardar bastante tiempo.

Para volcar los datos del informe

1. Haga clic en el nombre del informe.
2. Haga clic en el icono de puntos suspensivos vertical en la esquina superior derecha y, a continuación, en **Volcado de datos**.
3. Especifique la dirección de correo electrónico de los destinatarios.
4. En **Intervalo de tiempo**, especifique el intervalo de tiempo.
5. Haga clic en **Enviar**.

Resumen ejecutivo

El informe resumido ejecutivo presenta la información general del estado de la protección de los entornos de sus clientes y sus dispositivos protegidos para un intervalo de tiempo específico.

El informe resumido ejecutivo incluye secciones con widgets dinámicos que muestran parámetros de rendimiento claves relacionados con el uso por parte del cliente de los siguientes servicios en la nube: Copia de seguridad, protección contra malware, evaluación de vulnerabilidades, gestión de parches, prevención de pérdida de datos, certificación, recuperación ante desastres y File Sync & Share.

Puede personalizar el informe de diversas formas:

- Añadir o quitar secciones.
- Cambiar el orden de las secciones.
- Cambiar el nombre de secciones.
- Mover widgets de una sección a otra.
- Cambiar el orden de los widgets de cada sección.
- Añadir o quitar widgets.
- Personalizar widgets.

Puede generar informes resumidos ejecutivos en formato PDF y Excel y enviarlos a las partes interesadas o los dueños de las organizaciones de sus clientes para que puedan ver fácilmente el valor técnico y comercial de los servicios prestados.

Los administradores de socios solo pueden generar y enviar el informe resumido ejecutivo a clientes directos. En caso de una jerarquía de inquilinos más compleja que tenga subsocios, estos deberán generar el informe.

Widgets de resúmenes ejecutivos

Puede añadir o eliminar las secciones y widgets del informe resumido ejecutivo y controlar qué información incluir en él.

Widgets de resumen de cargas de trabajo

La siguiente tabla proporciona más información sobre los widgets de la sección **Resumen de cargas de trabajo**.

Widget	Descripción
Estado de la protección de las cargas de trabajo de la nube	Este widget muestra el número de cargas de trabajo de la nube protegidas y no protegidas por tipo en el momento en que se generó el informe. Las cargas de trabajo de la nube protegidas son aquellas a las que se les aplica, como mínimo, un plan de copias de seguridad. Las cargas de trabajo de la nube sin protección son aquellas a las que no se les aplica ningún plan de copias de seguridad. El gráfico muestra los siguientes tipos de carga de trabajo de la nube (en orden alfabético de la A a la Z): • Google Workspace: Drive • Gmail de Google Workspace

Widget	Descripción
	• Unidad compartida de Google Workspace • Buzones de correo de Hosted Exchange • Buzones de correo de Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Sitios web Para algunos tipos de carga de trabajo, se utilizan los siguientes grupos de cargas de trabajo: • Microsoft 365: Usuarios, grupos, carpeta públicas, equipos y colecciones de sitios • Google Workspace: Usuarios y unidades compartidas • Hosted Exchange: Usuarios Si un grupo de cargas de trabajo tiene más de 10 000 cargas de trabajo, el widget no mostrará ningún dato de las correspondientes cargas de trabajo. Por ejemplo, si el cliente tiene una cuenta de Microsoft 365 con 10 000 buzones de correo y un servicio de OneDrive para 500 usuarios, todos pertenecen al grupo de cargas de trabajo Usuarios. La suma de estas cargas de trabajo es 10 500, lo que excede el límite de 10 000 de un grupo de cargas de trabajo. Por lo tanto, el widget ocultará los correspondientes tipos de carga de trabajo: Buzones de correo de Microsoft 365 y Microsoft 365 OneDrive.
Resumen de ciberprotección	El widget muestra los parámetros clave del rendimiento de la ciberprotección para el periodo de tiempo especificado. **Datos en la copia de seguridad**: el tamaño total de los archivos comprimidos que se crearon en el almacenamiento local y en la nube. **Amenazas mitigadas**: el número total de malware bloqueado en los dispositivos. **URL maliciosas bloqueadas**: el número total de URL bloqueadas en todos los dispositivos. **Vulnerabilidades solucionadas**: el número total de vulnerabilidades solucionadas mediante la instalación de parches de software en todos los dispositivos. **Parches instalados**: el número total de parches instalados en todos los dispositivos. **Servidores protegidos por la recuperación ante desastres**: el número total de servidores protegidos por la recuperación ante desastres.

Widget	Descripción
	Usuarios de File Sync & Share: el número total de usuarios finales e invitados que utilizan Cyber Files. **Archivos certificados ante notario**: el número total de archivos certificados ante notario. **Documentos firmados electrónicamente**: el número total de documentos firmados electrónicamente. **Dispositivos periféricos bloqueados**: el número total de dispositivos periféricos bloqueados.
Estado de la red de las cargas de trabajo	Este widget muestra cuántas cargas de trabajo están aisladas y cuántas conectadas (el estado normal de la carga de trabajo). Seleccione el cliente correspondiente. La vista de la carga de trabajo mostrada se filtra para que aparezcan las cargas de trabajo aisladas. Haga clic en el valor Conectada para ver la Carga de trabajo con la lista de agentes filtrada para mostrar las cargas de trabajo conectadas (para el cliente seleccionado).
Estado de la protección de las cargas de trabajo	El widget muestra las cargas de trabajo protegidas y sin protección por tipo en el momento en que se generó el informe. Las cargas de trabajo protegidas son aquellas a las que se les aplica, como mínimo, un plan de protección o de copias de seguridad. Las cargas de trabajo sin protección son aquellas a las que no se les aplica ningún plan de protección ni de copias de seguridad. Se tienen en cuenta las siguientes cargas de trabajo: **Servidores**: servidores físicos y servidores de controladores de dominio. **Estaciones de trabajo**: estaciones de trabajo físicas. **Máquinas virtuales**: máquinas virtuales con agente y sin agente. **Servidores de alojamiento web**: servidores virtuales o físicos con cPanel o Plesk instalado. **Dispositivos móviles**: dispositivos móviles físicos. Una carga de trabajo puede pertenecer a más de una categoría. Por ejemplo, un servidor de alojamiento web se incluye en dos categorías: **Servidores** y **Servidores de alojamiento web**.
Estado de la protección de las cargas de trabajo de la nube	**Estado de la protección de las cargas de trabajo de la nube** El widget muestra el número de cargas de trabajo de la nube protegidas y no protegidas por tipo en el momento en que se generó el informe. Las cargas de trabajo de la nube protegidas son aquellas a las que se les aplica, como mínimo, un plan de copias de seguridad. Las cargas de trabajo de la nube sin protección son aquellas a las que no se les aplica ningún plan de copias de seguridad. El gráfico muestra los siguientes tipos de carga de trabajo de la nube (en orden alfabético de la A a la Z): • Google Workspace Drive

Widget	Descripción
	• Google Workspace Gmail • Google Workspace Shared Drive • Buzones de correo de Hosted Exchange • Buzones de correo de Microsoft 365 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • Sitios web Para algunos tipos de carga de trabajo, se utilizan los siguientes grupos de cargas de trabajo: • Microsoft 365: Usuarios, grupos, carpeta públicas, equipos y colecciones de sitios • Google Workspace: Usuarios y unidades compartidas • Hosted Exchange: Usuarios Si un grupo de cargas de trabajo tiene más de 10 000 cargas de trabajo, el widget no mostrará ningún dato de las correspondientes cargas de trabajo. Por ejemplo, si el cliente tiene una cuenta de Microsoft 365 con 10 000 buzones de correo y un servicio de OneDrive para 500 usuarios, todos pertenecen al grupo de cargas de trabajo Usuarios. La suma de estas cargas de trabajo es 10 500, lo que excede el límite de 10 000 de un grupo de cargas de trabajo. Por lo tanto, el widget ocultará los correspondientes tipos de carga de trabajo: Buzones de correo de Microsoft 365 y Microsoft 365 OneDrive.

Widgets de protección contra malware

La siguiente tabla proporciona más información sobre los widgets de la sección **Protección frente a amenazas**.

Widget	Descripción
Análisis antimalware de archivos	El widget muestra los resultados del análisis antimalware bajo demanda de los dispositivos para el intervalo de fechas especificado. **Archivos**: el número total de archivos escaneados **Limpios**: el número total de archivos limpios **Detectados, en cuarentena**: el número total de archivos infectados puestos en cuarentena **Detectados, sin cuarentena**: el número total de archivos infectados que no se han puesto en cuarentena **Dispositivos protegidos**: el número total de dispositivos con una política de

Widget	Descripción
	protección contra malware aplicada **Número total de dispositivos registrados**: el número total de dispositivos registrados en el momento en que se generó el informe
Análisis antimalware de copias de seguridad	El widget muestra los resultados del análisis antimalware de las copias de seguridad para el intervalo de fechas especificado mediante los siguientes parámetros: • Número total de puntos de recuperación analizados • Número de puntos de recuperación limpios • Número de puntos de recuperación limpios con particiones no admitidas • Número de puntos de recuperación infectados. Este parámetro incluye el número de puntos de recuperación infectados con particiones no admitidas.
URL bloqueadas	El widget muestra los resultados de URL bloqueadas agrupadas por categoría de sitio web para el intervalo de fechas especificado. El widget enumera las siete categorías de sitio web que tienen un mayor número de URL bloqueadas y combina el resto de categorías de sitio web en **Otros**. Para obtener más información acerca de las categorías de sitio web, consulte el tema de filtrado de URL en Cyber Protection.
Gráfico de quemado de incidentes de seguridad	Este widget muestra la tasa de eficiencia de incidentes cerrados de la empresa seleccionada; el número de incidentes abiertos se mide comparado con el número de incidentes cerrados en un periodo de tiempo. Mantenga el ratón encima de una columna para ver un desglose de los incidentes cerrados y abiertos del día seleccionado. El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.
Tiempo medio de reparación de incidentes	Este widget muestra el tiempo medio de reparación de incidentes de seguridad. Indica la rapidez con la que se investigan y reparan los incidentes. Haga clic en una columna para ver un desglose de incidentes según la gravedad (**Crítica**, **Alta** y **Media**) y una indicación sobre cuánto tardan en repararse los distintos niveles de gravedad. El valor % mostrado entre paréntesis indica el aumento o descenso en comparación con el periodo de tiempo anterior.
Estado de la amenaza	Este widget muestra el estado actual de la amenaza para las cargas de trabajo de una empresa (independientemente del número de cargas de trabajo) y destaca el número de incidentes que no se han mitigado y deben investigarse. El widget también indica el número de incidentes mitigados (de forma manual o automáticamente por el sistema).
Amenazas	El widget muestra el número de amenazas detectadas para el intervalo de

Widget	Descripción
detectadas por la tecnología de protección	fechas especificado, agrupadas por las siguientes tecnologías de protección: • Analizando antimalware • Motor de comportamiento • Protección ante criptominado • Prevención contra explotación • Protección activa contra ransomware • Protección en tiempo real • Filtrado de URL

Widgets de copias de seguridad

La siguiente tabla proporciona más información sobre los widgets de la sección **Copia de seguridad**.

Widget	Descripción
Cargas de trabajo en la copia de seguridad	El widget muestra el número total de cargas de trabajo registradas según el estado de la copia de seguridad. **Con copia de seguridad**: número de cargas de trabajo con copia de seguridad (al menos una copia de seguridad realizada con éxito) durante el intervalo de fechas del informe. **Sin copia de seguridad**: número de cargas de trabajo sin copia de seguridad (sin una copia de seguridad realizada con éxito) durante el intervalo de fechas del informe.
Estado del disco por dispositivo físico	El widget muestra el estado agregado de los dispositivos físicos según el estado de sus discos. **OK**: este estado del disco hace referencia a los valores [70-100]. El estado del dispositivo es **OK** cuando todos sus discos tienen el estado **OK**. **Advertencia**: este estado del disco hace referencia a los valores [30-70]. El estado de un dispositivo es **Advertencia** cuando el estado de al menos uno de sus discos es **Advertencia** y cuando no hay discos con el estado **Error**. **Error**: este estado del disco hace referencia a los valores [0-30]. El estado de un dispositivo es **Error** cuando el estado de al menos uno de sus discos es **Error**. **Calculando datos del disco**: el estado de un dispositivo es **Calculando datos del disco** cuando los estados de sus discos no se han calculado todavía.
Uso del almacenamiento	El widget muestra el número y el tamaño totales de las copias de seguridad en la nube y en el almacenamiento local para el intervalo de

Widget	Descripción
de copia de seguridad	tiempo especificado.

Widgets de evaluación de vulnerabilidades y gestión de parches

La siguiente tabla proporciona más información sobre los widgets de la sección **Evaluación de vulnerabilidades y gestión de parches**.

Widget	Descripción
Vulnerabilidades solucionadas	El widget muestra los resultados de rendimiento de la evaluación de vulnerabilidades para el intervalo de fechas especificado. **Total**: el número total de vulnerabilidades solucionadas. **Vulnerabilidades de software de Microsoft**: número total de vulnerabilidades de Microsoft solucionadas en todos los dispositivos Windows. **Vulnerabilidades de software de terceros para Windows**: el número total de vulnerabilidades de terceros para Windows solucionadas en todos los dispositivos Windows. **Cargas de trabajo analizadas**: el número total de dispositivos que se han analizado correctamente para buscar vulnerabilidades al menos una vez en el intervalo de fechas especificado.
Parches instalados	El widget muestra los resultados de rendimiento de la gestión de parches para el intervalo de fechas especificado. **Instalado**: el número total de parches que se han instalado correctamente en todos los dispositivos. **Parches de software de Microsoft**: el número total de parches de software de Microsoft que se han instalado en todos los dispositivos Windows. **Parches de software de terceros para Windows**: el número total de parches de software de terceros para Windows que se han instalado en todos los dispositivos Windows. **Cargas de trabajo solucionadas**: el número total de dispositivos que se han solucionado correctamente (con al menos un parche instalado correctamente durante el intervalo de fechas especificado).

Widgets de recuperación ante desastres

La siguiente tabla proporciona más información sobre los widgets de la sección **Recuperación ante desastres**.

Widget	Descripción
Estadísticas de recuperación ante desastres	El widget muestra los parámetros de rendimiento claves de la recuperación ante desastres para el intervalo de fechas especificado. **Conmutaciones por error de producción**: el número de operaciones de conmutación por error de producción para el intervalo de tiempo especificado. **Conmutaciones por error de prueba**: el número total de operaciones de conmutación por error de prueba ejecutadas durante el intervalo de tiempo especificado. **Servidores principales**: el número total de servidores principales en el momento en que se generó el informe. **Servidores de recuperación**: el número total de servidores de recuperación en el momento en que se generó el informe. **IP públicas**: el número total de direcciones IP públicas (en el momento en que se generó el informe). **Total de puntos de cálculo consumidos**: el número total de puntos de cálculo consumidos durante el intervalo de tiempo especificado.
Servidores de recuperación ante desastres probados	El widget muestra información sobre los servidores protegidos por la recuperación ante desastres y comprobados con la conmutación por error de prueba. El widget muestra los siguientes parámetros: **Servidor protegido**: el número de servidores protegidos por la recuperación ante desastres (servidores que tienen al menos un servidor de recuperación) en el momento en que se generó el informe. **Probado**: el número de servidores protegidos por la recuperación ante desastres que se comprobaron con la conmutación por error de prueba durante el intervalo de tiempo seleccionado de entre todos los servidores protegidos por la recuperación ante desastres. **No probado**: el número de servidores protegidos por la recuperación ante desastres que no se comprobaron con la conmutación por error de prueba durante el intervalo de tiempo seleccionado de entre todos los servidores protegidos por la recuperación ante desastres. El widget también muestra el tamaño del almacenamiento de la recuperación ante desastres (en GB) en el momento en que se generó el informe. Es la suma del tamaño de las copias de seguridad de los servidores en la nube.
Servidores protegidos con recuperación ante desastres	El widget muestra información sobre los servidores protegidos por la recuperación ante desastres y los servidores que no están protegidos. El widget muestra los siguientes parámetros:

Widget	Descripción
	El número total de servidores registrados en el inquilino de cliente en el momento en que se generó el informe. **Protegido**: el número de servidores protegidos por la recuperación ante desastres (tienen al menos un servidor de recuperación y una copia de seguridad del servidor completa) de entre todos los servidores registrados en el momento en que se generó el informe. **Sin protección**: el número total de servidores sin protección de entre todos los servidores registrados en el momento en que se generó el informe.

Widget para la prevención de pérdida de datos

El siguiente tema proporciona más información sobre los dispositivos periféricos bloqueados de la sección **Prevención de pérdida de datos**.

El widget muestra el número total de dispositivos bloqueados por tipo de dispositivo para el intervalo de fechas especificado.

- Almacenamiento extraíble
- Extraíble cifrada
- Impresoras
- Portapapeles: incluye los tipos de dispositivo de captura del Portapapeles y la Captura de pantalla.
- Dispositivos móviles
- Bluetooth
- Unidades ópticas
- Unidades de disquetes
- USB: incluye los tipos de dispositivo de puerto USB y puerto USB redirigido.
- FireWire
- Dispositivos asignados
- Portapapeles redirigido: incluye los tipos de dispositivo Entrada de portapapeles redirigida y Salida de portapapeles redirigida.

El widget muestra los primeros siete tipos de dispositivo con el mayor número de dispositivos bloqueados y combina el resto de tipos de dispositivos en el tipo **Otros**.

Widgets de File Sync & Share

La siguiente tabla proporciona más información sobre los widgets de la sección **File Sync & Share**.

Widget	Descripción
Estadísticas de File Sync & Share	El widget muestra los siguientes parámetros: **Almacenamiento total en la nube utilizado**: el uso del almacenamiento total de todos los usuarios. **Usuarios finales**: el número total de usuarios finales. **Almacenamiento medio utilizado por usuario final**: el almacenamiento medio utilizado por usuario final. **Usuarios invitados**: el número total de usuarios invitados.
Uso del almacenamiento de File Sync & Share por los usuarios finales	El widget muestra el número total de usuarios finales de File Sync & Share que usan el almacenamiento en los siguientes intervalos: • 0-1 GB • 1-5 GB • 5-10 GB • 10-50 GB • 50-100 GB • 100-500 GB • 500-1 TB • Más de 1 TB

Widgets de certificación

La siguiente tabla proporciona más información sobre los widgets de la sección **Certificación**.

Widget	Descripción
Estadísticas de Cyber Notary	El widget muestra los siguientes parámetros de certificación: **Almacenamiento en la nube utilizado para certificación**: el tamaño total del almacenamiento utilizado para servicios de certificación. **Archivos certificados ante notario**: el número total de archivos certificados ante notario. **Documentos firmados electrónicamente**: el número total de documentos y archivos firmados electrónicamente.
Archivos certificados en usuarios finales	Muestra el número total de archivos certificados ante notario para todos los usuarios finales. Los usuarios se agrupan según el número de archivos certificados que tengan. • Hasta 10 archivos • 11-100 archivos • 101-500 archivos • 501-1000 archivos • Más de 1000 archivos

Widget	Descripción
Documentos firmados electrónicamente por los usuarios finales	El widget muestra el número total de documentos y archivos firmados electrónicamente para todos los usuarios finales. Los usuarios se agrupan según el número de documentos y archivos firmados electrónicamente que tengan. • Hasta 10 archivos • 11-100 archivos • 101-500 archivos • 501-1000 archivos • Más de 1000 archivos

Configuración del informe resumido ejecutivo

Puede actualizar los ajustes del informe que se configuraron al crear el informe resumido ejecutivo.

Para actualizar la configuración del informe resumido ejecutivo

1. En la consola de gestión, vaya a **Informes** > **Resumen ejecutivo**.
2. Haga clic en el nombre del informe resumido ejecutivo que desee actualizar.
3. Haga clic en **Configuración**.
4. Cambie los valores de los campos según sea necesario.
5. Haga clic en **Guardar**.

Crear un informe resumido ejecutivo

Puede crear un informe resumido ejecutivo, obtener la vista previa de su contenido, configurar los destinatarios y programar su envío automático.

Para crear un informe resumido ejecutivo

1. En la consola de gestión, vaya a **Informes** > **Resumen ejecutivo**.
2. Haga clic en **Crear informe resumido ejecutivo**.
3. En **Nombre del informe**, escriba el nombre.
4. Seleccione los destinatarios del informe.
   - Si desea enviarlo a todos los clientes directos, seleccione **Enviar a todos los clientes directos**.
   - Si desea enviar el informe a clientes específicos
     a. Deseleccione **Enviar a todos los clientes directos**.
     b. Haga clic en **Seleccionar contactos**.
     c. Seleccione los clientes específicos. Puede utilizar la Búsqueda para encontrar un contacto

determinado fácilmente.

d. Haga clic en **Seleccionar**.

5. Seleccione el intervalo: **30 días** o **Este mes**
6. Seleccione el formato del archivo: **PDF**, **Excel**, o **Excel y PDF**.
7. Configure la programación.
   - Si desea enviar el informe a los destinatarios en una fecha y hora específicas:
     a. Habilite la opción **Programado**.
     b. Haga clic en el campo **Día del mes**, borre el campo Último día y haga clic en la fecha que desee establecer.
     c. En el campo **Hora**, introduzca la hora a la que desee enviarlo.
     d. Haga clic en **Aplicar**.
   - Si desea crear el informe sin enviarlo a los destinatarios, deshabilite la opción **Programado**.
8. Haga clic en **Guardar**.

Personalizar un informe resumido ejecutivo

Puede determinar qué información incluir en el informe resumido ejecutivo. Puede añadir o quitar secciones o widgets, cambiar el nombre a secciones, personalizar widgets y arrastrar y soltar widgets y secciones para cambiar el orden en que la información aparece en el informe.

Para añadir una sección

1. Haga clic en **Agregar elemento** > **Agregar sección**.
2. En la ventana **Agregar sección**, escriba un nombre de sección o utilice el nombre de sección predeterminado.
3. Haga clic en **Añadir al informe**.

Para cambiar el nombre de una sección

1. En la sección a la que quiere cambiarle al nombre, haga clic en **Editar**.
2. En la ventana **Editar sección**, escribe el nuevo nombre.
3. Haga clic en **Guardar**.

Para eliminar una sección

1. En la sección que quiere eliminar, haga clic en **Eliminar sección**.
2. En la ventana de confirmación **Eliminar sección**, haga clic en **Eliminar**.

Para añadir un widget con configuración predeterminada a una sección

1. En la sección a la que quiere añadir el widget, haga clic en **Añadir widget**.
2. En la ventana **Añadir widget**, haga clic en el widget que quiera añadir.

Para añadir un widget personalizado a una sección

1. En la sección a la que quiere añadir el widget, haga clic en **Añadir widget**.
2. En la ventana **Añadir widget**, busque el widget que quiera añadir y haga clic en **Personalizar**.
3. Configure los campos según sea necesario.
4. Haga clic en **Añadir widget**.

Para añadir un widget con configuración predeterminada al informe

1. Haga clic en **Agregar elemento** > **Agregar widget**.
2. En la ventana **Añadir widget**, haga clic en el widget que quiera añadir.

Para añadir un widget personalizado al informe

1. Haga clic en **Añadir widget**.
2. En la ventana **Añadir widget**, busque el widget que quiera añadir y haga clic en **Personalizar**.
3. Configure los campos según sea necesario.
4. Haga clic en **Añadir widget**.

Para restablecer la configuración predeterminada de un widget

1. Haga clic en **Editar** en el widget que quiera personalizar.
2. Haga clic en **Restablecer valores predeterminados**.
3. Haga clic en **Realizado**.

Pasos para personalizar un widget

1. Haga clic en **Editar** en el widget que quiera personalizar.
2. Edite los campos según sea necesario.
3. Haga clic en **Realizado**.

Enviar informes resumidos ejecutivos

Puede enviar un informe resumido ejecutivo bajo demanda. En este caso, no se tiene en cuenta el ajuste **Programado** y el informe se envía inmediatamente. Cuando envía el informe, el sistema utiliza los valores de los destinatarios, el intervalo y el formato de archivo que están configurados en **Configuración**. Puede modificar esta configuración manualmente antes de enviar el informe. Para obtener más información, consulte "Configuración del informe resumido ejecutivo" (p. 120).

Pasos para enviar un informe resumido ejecutivo

1. En el portal de gestión, vaya a **Informes** > **Resumen ejecutivo**.
2. Haga clic en el nombre del informe resumido ejecutivo que desee enviar.
3. Haga clic en **Enviar ahora**.
   El sistema envía el informe resumido ejecutivo a los destinatarios seleccionados.

Zonas horarias de los informes

Las zonas horarias que se utilizan en los informes varían en función del tipo de informe. En la siguiente tabla encontrará información que le servirá como referencia.

Ubicación y tipo de informe	Zona horaria utilizado en el informe
Portal de administración > Información general > Operaciones (widgets)	La hora de la generación del informe es la de la zona horaria del equipo en el que se está ejecutando el navegador.
Portal de administración > Información general > Operaciones (exportado en PDF o xslx)	• La marca de fecha y hora del informe exportado es la de la zona horaria del equipo que se utilizó para exportar informe. • La zona horaria de las actividades que aparecen en el informe es UTC.
Portal de administración > Informes > Uso > Informes planificados	• El informe se genera a las 23:59:59 UTC el primer día del mes. • El informe se envía el segundo día del mes.
Portal de administración > Informes > Uso > Informes personalizados	La zona horaria y la fecha del informe es UTC.
Portal de administración > Informes > Operaciones (widgets)	• La hora de la generación del informe es la de la zona horaria del equipo en el que se está ejecutando el navegador. • La zona horaria de las actividades que aparecen en el informe es UTC.
Portal de administración > Informes > Operaciones (exportado en PDF o xslx)	• La marca de fecha y hora del informe exportado es la de la zona horaria del equipo que se utilizó para exportar informe. • La zona horaria de las actividades que aparecen en el informe es UTC.
Portal de administración > Informes > Operaciones (entrega planificada)	• La zona horaria de entrega del informe es UTC. • La zona horaria de las actividades que aparecen en el informe es UTC.
Portal de administración > Usuarios > Resumen diario de alertas activas	• Este informe se envía una vez al día entre las 10:00 y las 23:59 UTC. La hora a la que se envía el informe depende de la carga de trabajo del centro de datos. • La zona horaria de las actividades que aparecen en el informe es UTC.

Portal de administración > Usuarios > notificaciones de estado de ciberprotección	• Este informe se envía cuando finaliza una actividad. **Nota** En función de la carga de trabajo del centro de datos, es posible que algunos informes se entreguen con retraso. • La zona horaria de la actividad del informe es UTC.

Datos informados según el tipo de widget

Según el rango de datos que muestran, hay dos tipos de widgets en el panel de control:

- Widgets que muestran los datos reales en el momento de la navegación o la generación de informes.
- Widgets que muestran datos históricos.

Cuando configure un rango de fechas en los ajustes del informe para volcar datos para un periodo determinado, el rango de tiempo seleccionado se aplicará solo a los widgets que muestran datos históricos. El parámetro del rango de tiempo no se aplica a los widgets que muestran los datos reales en el momento de la navegación.

La siguiente tabla enumera los widgets disponibles y sus rangos de datos.

Nombre del widget	Datos mostrados en el widget e informes
#CyberFit Score por equipo	Reales
5 últimas alertas	Reales
Detalles de las alertas activas	Reales
Resumen de alertas activas	Reales
Actividades	Históricos
Lista de actividades	Históricos
Historial de alertas	Históricos
Análisis antimalware de copias de seguridad	Históricos
Análisis antimalware de archivos	Históricos
Detalles del análisis de copias de seguridad (amenazas)	Históricos
Estado de la copia de seguridad	Históricos: en columnas **Ejecuciones totales** y **Número de ejecuciones correctas** Reales: en el resto de columnas
Uso del almacenamiento de copia de	Históricos

seguridad	
Dispositivos periféricos bloqueados	Históricos
URL bloqueadas	Reales
Aplicaciones de Cloud	Reales
Estado de la protección de las cargas de trabajo de la nube	Reales
Cyber protection	Reales
Resumen de ciberprotección	Históricos
Mapa de protección de datos	Históricos
Dispositivos	Reales
Servidores de recuperación ante desastres probados	Históricos
Estadísticas de recuperación ante desastres	Históricos
Equipos detectados	Reales
Resumen del estado del disco	Reales
Estado del disco	Reales
Estado del disco por dispositivos físicos	Reales
Documentos firmados electrónicamente por los usuarios finales	Reales
Vulnerabilidades existentes	Históricos
Estadísticas de File Sync & Share	Reales
Uso del almacenamiento de File Sync & Share por los usuarios finales	Reales
Cambios del hardware	Históricos
Detalles del hardware	Reales
Inventario de hardware	Reales
Resumen de alertas histórico	Históricos
Resumen de ubicaciones	Reales
Actualizaciones que faltan por categoría	Reales
Sin protección	Reales

Archivos certificados en usuarios finales	Reales
Estadísticas de Notary	Reales
Historial de instalación de parches	Históricos
Estado de instalación del parche	Históricos
Resumen de la instalación del parche	Históricos
Vulnerabilidades solucionadas	Históricos
Parches instalados	Históricos
Estado de la protección	Reales
Elementos afectados recientemente	Históricos
Sesiones remotas	Históricos
Gráfico de quemado de incidentes de seguridad	Históricos
Tiempo medio de reparación de incidentes de seguridad	Históricos
Servidores protegidos con recuperación ante desastres	Reales
Inventario de software	Reales
Información general del software	Históricos
Estado de la amenaza	Reales
Amenazas detectadas por la tecnología de protección	Históricos
Distribución de los principales incidentes por carga de trabajo	Reales
Equipos vulnerables	Reales
Estado de la red de las cargas de trabajo	Reales
Cargas de trabajo en la copia de seguridad	Históricos
Estado de la protección de las cargas de trabajo	Reales

Registro de control

Para ver el registro de control, haga clic en **Registro de control**.

El registro de control proporciona un registro cronológico de los eventos siguientes:

- Operaciones realizadas por los usuarios en el portal de gestión
- Operaciones con recursos de la nube a la nube ejecutadas por los usuarios en la consola de servicio de Cyber Protection
- Las operaciones de secuencia de comandos cibernética realizadas por los usuarios en la consola de servicio de Cyber Protection
- Sistema de mensajes sobre el cumplimiento de cuotas y el uso de estas

El registro muestra eventos del inquilino en la que esté operando, así como de sus inquilinos secundarios. Puede hacer clic en un evento para ver más información sobre este.

Los registros de control se almacenan en el centro de datos y su disponibilidad no puede verse afectada por problemas relacionados con los equipos de usuarios finales.

El registro se borra a diario. Los eventos se eliminan tras 180 días.

Campos del registro de control

El registro muestra la siguiente información para cada evento:

- **Evento**
  Descripción breve del evento. Por ejemplo, **Se ha creado un inquilino**, **Se ha eliminado un inquilino**, **Se ha creado un usuario**, **Se ha eliminado un usuario**, **Se ha alcanzado la cuota**, **Se ha examinado el contenido de la copia de seguridad** o **Se ha cambiado la secuencia de comandos**.
- **Gravedad**
  Puede ser una de las opciones siguientes:
  - **Error**
    Indica un error.
  - **Advertencia**
    Indica una acción potencialmente negativa. Por ejemplo, **Se ha eliminado un inquilino**, **Se ha eliminado un usuario** o **Se ha alcanzado la cuota**.
  - **Aviso**
    Indica que es posible que un evento requiera atención. Por ejemplo, **Se ha actualizado un inquilino** o **Se ha actualizado un usuario**.
  - **Informativo**
    Indica una acción o un cambio informativo neutral. Por ejemplo, **Se ha creado un inquilino**, **Se ha creado un usuario**, **Se ha actualizado la cuota** o **Se ha eliminado el plan de programación**.
- **Fecha**
  La fecha y la hora en las que ocurrió el evento.
- **Nombre del objeto**
  El objeto con el que se realizó la operación. Por ejemplo, el objeto del evento **Se ha actualizado un usuario** es el usuario cuyas propiedades se modificaron. En el caso de los eventos relacionados con una cuota, dicha cuota sería el objeto.

- **Inquilino**

  El nombre del inquilino al que pertenece el objeto.
- **Iniciador**

  El inicio de sesión del usuario que inició el evento. En el caso de mensajes del sistema y eventos iniciados por los administradores de nivel superior, el iniciador se muestra como **Sistema**.
- **Inquilino del iniciador**

  El nombre del inquilino al que pertenece el iniciador. En el caso de mensajes del sistema y eventos iniciados por los administradores de nivel superior, el campo está vacío.
- **Método**

  Muestra si el evento se inició a través de la interfaz web o la API.
- **IP**

  Dirección IP del equipo desde el que se inició el evento.

Filtrado y búsqueda

Puede filtrar los eventos por tipo, gravedad o fecha. También puede buscarlos por nombre, objeto, inquilino, iniciador o inquilino del iniciador.

Paquetes Advanced Protection

Los paquetes de protección avanzada pueden activarse de manera adicional al servicio Protección y están sujetos a costes adicionales. Los paquetes de protección avanzada proporcionan una funcionalidad única que no se superpone con el conjunto de características estándar ni con otros paquetes avanzados. Los clientes pueden proteger sus cargas de trabajo con uno, varios o todos los paquetes avanzados. Los paquetes de protección avanzada están disponibles para los modos de facturación por carga de trabajo y por gigabyte del servicio Protección.

Se pueden habilitar las funciones avanzadas de File Sync & Share en este servicio. Está disponible en los modos de facturación por gigabyte y por usuario.

Puede activar los siguientes paquetes de protección avanzada:

- Copia de seguridad avanzada
- Gestión avanzada
- Seguridad avanzada
- Seguridad avanzada + EDR
- Prevención avanzada de la pérdida de datos
- Recuperación ante desastres avanzada
- Protección de correo electrónico avanzada
- File Sync & Share avanzado

Nota
Los paquetes avanzados solo se pueden utilizar cuando la característica que amplían está activada. Los usuarios no pueden utilizar las características avanzadas cuando la característica estándar del servicio está desactivada. Por ejemplo, los usuarios no pueden utilizar las características del paquete Advanced Backup si la característica Protección está desactivada.

Si tiene activado algún paquete de protección avanzada, sus características se mostrarán en el plan de protección marcadas con el icono de función avanzada. Al intentar activar la función, se avisará a los usuarios de que se aplicarán tasas adicionales.

Si no tiene activado algún paquete de protección avanzada, pero la venta de productos de gama superior está activada, las características de protección avanzada se mostrarán en el plan de protección, pero no se podrán utilizar. Aparecerá este icono junto al nombre de la característica. Se les mostrará un mensaje a los usuarios para que contacten con su administrador para activar el conjunto de características avanzado que necesiten.

Si no tiene activado algún paquete de protección avanzada y la venta de productos de gama superior está desactivada, los clientes no verán las características avanzadas en sus planes de protección.

Características y paquetes avanzados incluidos en los servicios de Cyber Protect

Cuando activa un servicio o conjunto de características en Cyber Protect, activa un número de características incluidas y disponibles de forma predeterminada. Además, puede activar paquetes de protección avanzada.

Las siguientes secciones contienen un resumen de gran nivel de las características y los paquetes avanzados del servicio Cyber Protect. Para ver una lista completa de ofertas, consulte la Guía de permisos de Cyber Protect.

Características avanzadas incluidas en el servicio de protección

Características avanzadas incluidas en el servicio de protección

Grupo de características	Características estándar incluidas	Características avanzadas
Seguridad	• #CyberFit Score • Evaluación de vulnerabilidades • Protección contra ransomware: Active Protection • Protección antivirus y antimalware: Detección de archivos en la nube basada en firmas (no hay protección en tiempo real, solo análisis programado)* • Protección antivirus y antimalware: Analizador de archivos basado en IA de ejecución previa, motor cibernético basado en el comportamiento • Administración de Microsoft Defender * Para detectar ataques de día cero, Cyber Protect utiliza reglas y algoritmos de análisis heurísticos para buscar comandos maliciosos.	Hay dos paquetes de protección avanzada disponibles: **Seguridad avanzada** y **Seguridad avanzada + EDR**. El paquete Advanced Security incluye lo siguiente: • Protección antivirus y antimalware con detección basada en firmas locales (con protección en tiempo real) • Prevención contra explotación • Filtrado de URL • Gestión de firewall de endpoint • Copia de seguridad forense, análisis de copias de seguridad en busca de malware, recuperación segura, lista blanca corporativa • Planes de protección inteligentes (integración con alertas del CPOC) • Análisis de copia de seguridad centralizado para malware • Borrado remoto El paquete de protección Seguridad avanzada + EDR incluye todas las características anteriores y las siguientes capacidades de detección y respuesta de

Grupo de características	Características estándar incluidas	Características avanzadas
		endpoints para identificar amenazas avanzadas o ataques en progreso: • Gestionar incidentes en una página de incidentes centralizada • Visualizar el ámbito y el impacto de los incidentes • Recomendaciones y medidas de corrección • Comprobar si hay ataques de dominio público en sus cargas de trabajo utilizando las fuentes de amenazas • Almacenar los eventos de seguridad durante 180 días Para obtener más información sobre cómo habilitar Seguridad avanzada + EDR, consulte "Habilitar Seguridad avanzada + EDR" (p. 136).
Prevención de pérdida de datos	• Control de dispositivos	• Prevención consciente del contenido de la pérdida de datos de cargas de trabajo a través de dispositivos periféricos y comunicación de red • Detección automática prediseñada de la información de identificación personal (PII), la información de salud protegida (PHI) y los datos del Estándar de Seguridad de los Datos para la Industria de Tarjetas de Pago (PCI DSS), así como de los documentos de la categoría "Marcado como confidencial" • Creación de la directiva de prevención de pérdida de datos automática con asistencia del usuario final opcional • Aplicación de la prevención de pérdida de datos adaptada con ajuste automático de directivas basado en el aprendizaje • Registro de auditoría centralizado basado en la nube, alertas y notificaciones de usuario final

Grupo de características	Características estándar incluidas	Características avanzadas
Gestión	• Gestión de grupo de las cargas de trabajo • Gestión centralizada de los planes de protección • Inventario de hardware • Control remoto • Acciones remotas • Conexiones simultáneas por técnico • Protocolo de conexión remota: RDP	• Gestión de parches • Estado del disco • Inventario de software • Corrección segura del archivo • Secuencia de comandos cibernética • Asistencia remota • Transferencia y uso compartido de archivos • Selección de una sesión para conectarse • Observar las cargas de trabajo en la vista múltiple • Modos de conexión: controlar, observar y cortina • Conexión mediante la aplicación Quick Assist • Protocolos de conexión remota: NEAR y uso compartido de pantalla • Grabación de la sesión para conexiones NEAR • Transmisión de captura de pantalla • Informe de historial de sesiones
Seguridad del correo electrónico	Ninguno	Protección en tiempo real de sus buzones de correo de Microsoft 365 y Gmail: • Antimalware Antispam • Análisis de URL en correos electrónicos • Análisis de DMARC • Antisuplantación • Protección contra la suplantación de identidad • Análisis de adjuntos • Supresión y reconstrucción de contenido • Gráfico de confianza Consulte la guía de configuración.
Cyber Disaster Recovery Cloud	Puede utilizar las características estándar de la recuperación ante desastres para probar los escenarios de	Puede activar el paquete Advanced Disaster Recovery y proteger sus cargas de trabajo mediante el uso de la

Grupo de características	Características estándar incluidas	Características avanzadas
	recuperación ante desastres para sus cargas de trabajo. Tenga en cuenta las características estándar de Disaster Recovery que están disponibles y sus límites: • Pruebe la conmutación por error en un entorno de red aislado. Está limitada a 32 puntos de cálculo al mes y hasta 5 operaciones de conmutación por error de prueba a la vez. • Configuración del servidor de recuperación: 1 CPU y 2 GB de RAM, 1 CPU y 4 GB de RAM y 2 CPU y 8 GB de RAM. • Número de puntos de recuperación disponibles por conmutación por error: solo el último punto de recuperación disponible justo después de una copia de seguridad. • Modos de conectividad disponibles: Solo en la nube y de punto a sitio. • Disponibilidad de la puerta de enlace de VPN: La puerta de enlace de VPN se suspenderá de manera temporal si permanece inactiva durante 4 horas después de completarse la última conmutación por error de prueba y se implementará de nuevo cuando inicie una conmutación por error de prueba. • Número de redes en la nube: 1. • Acceso a Internet • Operaciones con runbooks: crear y editar.	funcionalidad completa de Disaster Recovery. Tenga en cuenta las características avanzadas de Disaster Recovery que están disponibles: • Conmutación por error de producción • Pruebe la conmutación por error en un entorno de red aislado. • Número de puntos de recuperación disponibles para la conmutación por error: todos los puntos de recuperación que están disponibles después de crear el servidor de recuperación. • Servidores principales • Configuración del servidor de recuperación y del principal: Sin limitaciones • Modos de conectividad disponibles: Solo en la nube, de punto a sitio, OpenVPN de sitio a sitio y VPN de IPsec de varios sitios. • Disponibilidad de la puerta de enlace de VPN: disponible siempre. • Número de redes en la nube: 23. • Direcciones IP públicas • Acceso a Internet • Operaciones con runbooks: crear, editar y ejecutar.

Características avanzadas y de pago por uso en el servicio de protección

Características avanzadas y de pago por uso en el servicio de protección

Grupo de características	Características de pago por uso	Características avanzadas
Copia de seguridad	• Copia de seguridad del archivo • Copia de seguridad de imagen • Copia de seguridad de aplicaciones • Copia de seguridad de los recursos compartidos de red • Copia de seguridad en el almacenamiento en la nube • Copia de seguridad en almacenamiento local **Nota** Se aplican tasas por el uso del almacenamiento en la nube.	• Clústeres de Microsoft SQL Server y Microsoft Exchange Server • Oracle DB • SAP HANA • Mapa de protección de datos • Protección de datos continua • Planes de procesamiento de datos fuera del host • Certificación de las copias de seguridad • Usuarios de Microsoft 365 • Licencias de Google Workspace
File Sync & Share	• Almacene contenido cifrado basado en archivos • Sincronice archivos entre todos sus dispositivos designados • Comparta carpetas y archivos con personas y sistemas designados	• Certificación y firma electrónica • Plantillas de documentos* * Copia de seguridad de archivos de sincronización y uso compartido
Envío de datos físicos	Función de envío de datos físicos	N/D
Notary	• Certificación de archivos • Firma electrónica de archivos • Plantillas de documento	N/D

Nota
No puede activar paquetes de protección avanzada sin activar la característica de protección estándar que amplían. Si desactiva una característica, sus paquetes avanzados se desactivarán automáticamente y los planes de protección que utilizan se revocarán de forma automática. Por ejemplo, si desactiva la característica de protección, sus paquetes avanzados se desactivarán automáticamente y todos los planes que utilizan se revocarán.

Los usuarios no pueden utilizar paquetes de protección avanzada sin tener la protección estándar, pero pueden utilizar solo las características incluidas en la protección estándar junto con los paquetes avanzados en las cargas de trabajo específicas. En este caso, solo se les cobrará por los paquetes avanzados que utilicen.

Para más información acerca de la facturación, consulte "Modos de facturación para Cyber Protect" (p. 8).

Prevención avanzada de la pérdida de datos

La prevención avanzada de la pérdida de datos previene la pérdida de información confidencial de las estaciones de trabajo, servidores y máquinas virtuales mediante la inspección del contenido de los datos transferidos a través de canales locales y de red y la aplicación de la política de flujos de datos específicos de la organización.

Antes de empezar a utilizar el módulo de prevención avanzada de la pérdida de datos, compruebe que lee y entiende los conceptos básicos y la lógica de la gestión de la prevención avanzada de la pérdida de datos descritos en la Guía de fundamentos.

Puede que también desee revisar el documento de Especificaciones técnicas.

Habilitar la prevención avanzada de la pérdida de datos

De forma predeterminada, se ha habilitado la prevención avanzada de la pérdida de datos en la configuración para los nuevos inquilinos. Si se ha deshabilitado la funcionalidad durante el proceso de creación del inquilino, los administradores de partners pueden habilitarla más tarde.

Pasos para habilitar la prevención avanzada de la pérdida de datos

1. En la consola de gestión de Cyber Protect Cloud, vaya a **Clientes**.
2. Seleccione el inquilino a editar.
3. En la sección **Seleccionar servicios**, desplácese a **Protección** y en el modo de facturación que aplique, seleccione **Prevención avanzada de la pérdida de datos**.
4. En Configurar servicios, desplácese a **Prevención avanzada de la pérdida de datos** y configure las cuotas.
   De forma predeterminada, la cuota se establece en ilimitada.
5. Guarde la configuración.

Seguridad avanzada + EDR

La detección y respuesta de endpoints (EDR) detecta actividad sospechosa en la carga de trabajo, incluidos los ataques que han pasado desapercibidos, y genera incidentes. Estos incidentes proporcionan información general paso a paso de cada ataque, lo que le ayuda a entender cómo ocurrió un ataque y cómo impedir que vuelva a ocurrir. Gracias a las interpretaciones fáciles de entender de cada fase del ataque, el tiempo invertido en investigar ataques puede reducirse a unos pocos minutos.

Habilitar Seguridad avanzada + EDR

Como administrador de partner, puede habilitar el paquete de protección Seguridad avanzada + EDR para proporcionar la funcionalidad de detección y respuesta de endpoints (EDR) en los planes de protección de clientes.

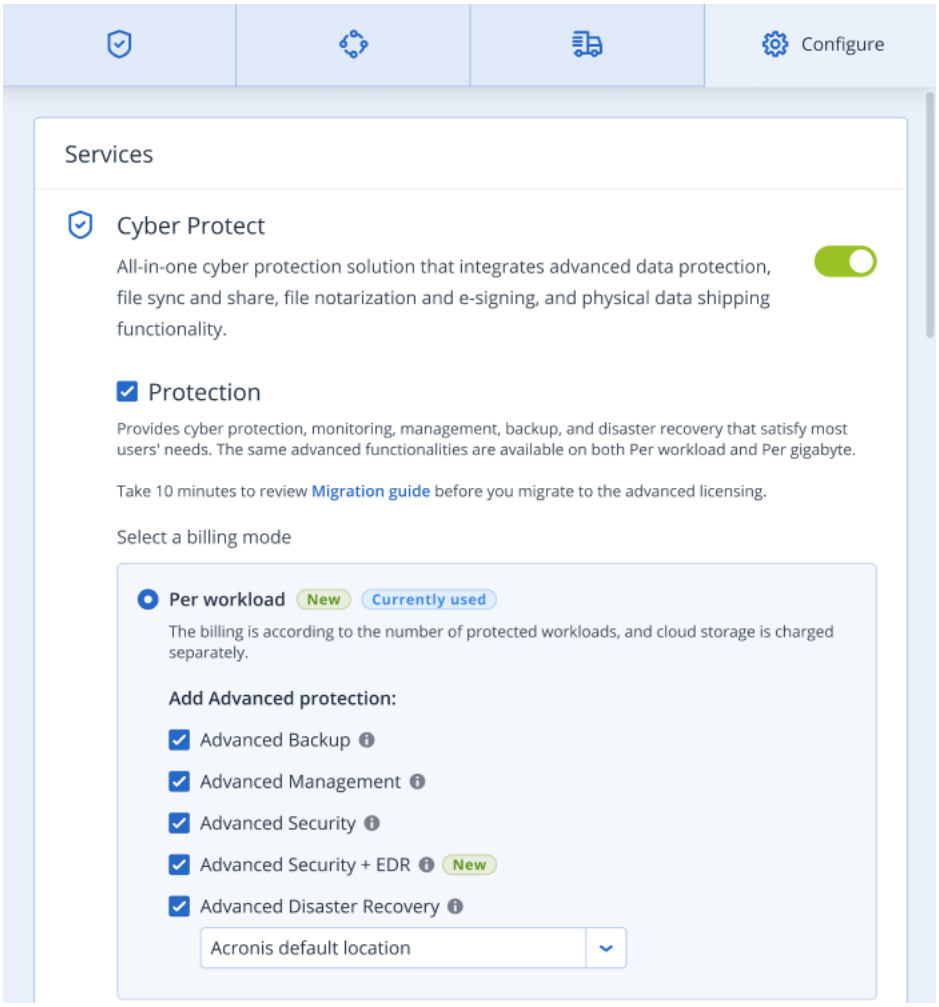
Pasos para habilitar el paquete Seguridad avanzada + EDR

1. Inicie sesión en el portal de gestión.

   Nota
   Si se le solicita, seleccione los clientes a los que desea aplicar el paquete de protección Seguridad Avanzada + EDR y haga clic en **Habilitar**.

2. En el panel de navegación izquierdo, haga clic en **CLIENTES**.
3. En Cyber Protect, haga clic en la pestaña **Protección**.
   Se mostrará la lista de clientes existentes suscritos al servicio de protección.
4. Haga clic en el cliente al que desea añadir el paquete Seguridad Avanzada + EDR.
   En la pestaña, **Configurar**, en la sección Protección, asegúrese de que la casilla de verificación

Seguridad Avanzada + EDR está seleccionada.



Recuperación ante desastres avanzada

Puede activar el paquete Advanced Disaster Recovery y proteger sus cargas de trabajo mediante el uso de la funcionalidad completa de Disaster Recovery.

Están disponibles las siguientes características de recuperación avanzada ante desastres:

- Conmutación por error de producción
- Pruebe la conmutación por error en un entorno de red aislado.
- Número de puntos de recuperación disponibles para la conmutación por error: todos los puntos de recuperación que están disponibles después de crear el servidor de recuperación.
- Servidores principales
- Configuración del servidor de recuperación y del principal: Sin limitaciones
- Modos de conectividad disponibles: Solo en la nube, de punto a sitio, OpenVPN de sitio a sitio y VPN de IPsec de varios sitios.
- Disponibilidad de la puerta de enlace de VPN: disponible siempre.

- Número de redes en la nube: 23.
- Direcciones IP públicas
- Acceso a Internet
- Operaciones con runbooks: crear, editar y ejecutar.

Protección de correo electrónico avanzada

El paquete Advanced Email Security protege en tiempo real sus buzones de correo de Microsoft 365, Google Workspace u Open-Xchange:

- Antimalware y antispam
- Análisis de URL en correos electrónicos
- Análisis de DMARC
- Antisuplantación
- Protección contra la suplantación de identidad
- Análisis de adjuntos
- Supresión y reconstrucción de contenido
- Gráfico de confianza

Obtenga más información acerca de Advanced Email Security en la ficha técnica de Advanced Email Security.

Para obtener indicaciones sobre la configuración, consulte Advanced Email Security con Perception Point.

Integraciones

Integración con sistemas externos

Un proveedor de servicios puede integrar Cyber Protect Cloud con un sistema de terceros de la siguiente manera:

- Mediante la configuración de una extensión de la plataforma en este sistema.

  En la página **Integración** del portal de administración aparecen las extensiones disponibles para los sistemas más populares de Automatización de Servicios Profesionales (PSA) y Gestión y Monitorización Remota (RMM).

  Esta es la forma recomendada de integrar la plataforma.
- Mediante la creación de un cliente API para el sistema y, por lo tanto, habilitando al sistema para que pueda acceder a las interfaces de programación de aplicaciones (API) de la plataforma y a sus servicios. Los clientes API forman parte del marco de autorización OAuth 2.0 de la plataforma. Para obtener más información sobre OAuth 2.0, consulte https://tools.ietf.org/html/rfc6749.

  Esta es una forma de bajo nivel de integrar la plataforma que requiere habilidades de programación. Le recomendamos que se decante por ella cuando no haya ninguna extensión de la plataforma para el sistema o bien si el sistema se va a personalizar para determinadas situaciones de administración de la plataforma y de sus servicios que no se incluyan en la extensión disponible.

Configuración de una integración de Cyber Protect Cloud

1. Inicie sesión en el portal de gestión.
2. En el menú de navegación principal, vaya a **Integraciones**.
3. Haga clic en el nombre del sistema de terceros con el que desea habilitar la integración.
4. Siga las instrucciones que aparecen en pantalla.

Puede encontrar más información sobre las integraciones disponibles con sistemas externos, incluida la documentación paso a paso, en https://solutions.acronis.com.

Gestión de clientes API

Se pueden integrar sistemas de terceros con Cyber Protect Cloud mediante interfaces de programación de aplicaciones (API). El acceso a estas API se habilita mediante clientes API, una parte integral del marco de autorización OAuth 2.0 de la plataforma.

¿Qué es un cliente API?

Un cliente API es una cuenta especial de una plataforma cuya función es representar a un sistema de terceros que se tiene que autenticar y autorizar para acceder a los datos de las API de la

plataforma y sus servicios.

El acceso del cliente está limitado a un inquilino, en el que un administrador crea al cliente y a sus subinquilinos.

Al crearse, el cliente hereda los roles de servicio de la cuenta administrador, que no se pueden cambiar posteriormente. El hecho de que cambien los roles de la cuenta de administrador o que se deshabiliten no afecta al cliente.

Las credenciales del cliente están formadas por el identificador único (ID) y un valor secreto. Las credenciales no caducan y no se pueden utilizar para iniciar sesión en el portal de administración ni en ninguna consola de servicio. El valor secreto se puede restablecer.

No es posible habilitar la autenticación de doble factor para el cliente.

Proceso de integración habitual

1. Un administrador crea un cliente API en un inquilino que gestionará un sistema de terceros.
2. El administrador habilita el flujo de credenciales del cliente OAuth 2.0 en el sistema de terceros.
   Según este flujo, antes de acceder al inquilino y sus servicios a través de la API, el sistema debe usar la API de autorización para enviar las credenciales del cliente creado a la plataforma. La plataforma genera y devuelve un token de seguridad, la única cadena críptica asignada a este cliente concreto. A continuación, el sistema debe añadir este token a todas las solicitudes a la API.
   Un token de seguridad acaba con la necesidad de mandar las credenciales del cliente con las solicitudes a la API. Para obtener un nivel mayor de seguridad, el token expira en dos horas. Cuando pase este tiempo, todas las solicitudes a la API con el toque expirado fallarán y el sistema tendrá que solicitar uno nuevo a la plataforma.

Para obtener más información sobre cómo usar las API de plataforma y autorización, consulte la guía del desarrollador en https://developer.acronis.com/doc/account-management/v2/guide/index.

Creación de un cliente API

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Ajustes** > **Clientes API** > **Crear cliente API**.
3. Introduzca un nombre para el cliente API.
4. Haga clic en **Siguiente**.
   De forma predeterminada, el cliente API se crea con el estado **Habilitado**.
5. Copie y guarde el ID, el valor secreto del cliente y la URL del centro de datos. Los necesitará para habilitar el flujo de credenciales del cliente OAuth 2.0 en el sistema de terceros.

   Importante
   Por motivos de seguridad, la clave solo se muestra una vez. No hay ninguna forma de recuperar

este valor si lo pierde, la única opción es restablecerlo.

6. Haga clic en **Realizado**.

Restablecimiento del valor secreto de un cliente API

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Ajustes** > **Clientes API**.
3. En la lista, busque el cliente que necesite.
4. Haga clic en y luego en **Restablecer secreto**.
5. Para confirmar su decisión, haga clic en **Siguiente**.
   Se generará un nuevo valor secreto. El ID del cliente y la URL del centro de datos no cambiarán.
   Todos los tokens de seguridad asignados a este cliente expirarán inmediatamente y fallarán las solicitudes a la API con estos clientes.
6. Copie y guarde el nuevo valor secreto del cliente.

   Importante
   Por motivos de seguridad, la clave solo se muestra una vez. No hay ninguna forma de recuperar este valor si lo pierde, la única opción es restablecerlo.

7. Haga clic en **Realizado**.

Deshabilitación de un cliente API

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Ajustes** > **Clientes API**.
3. En la lista, busque el cliente que necesite.
4. Haga clic en y en **Deshabilitar**.
5. Confirme su decisión.
   El estado del cliente cambiará a **Deshabilitado**.
   Las solicitudes a la API con tokens de seguridad que estén asignadas a este cliente fallarán, pero los tokens no caducarán inmediatamente. El hecho de deshabilitar el cliente no afecta a la fecha de caducidad de los tokens.
   El cliente se podrá volver a habilitar en cualquier momento.

Habilitación de un cliente API deshabilitado

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Ajustes** > **Clientes API**.

3. En la lista, busque el cliente que necesite.
4. Haga clic en y en **Habilitar**.

   El estado del cliente cambiará a **Activo**.

   Las solicitudes a la API con tokens de seguridad que estén asignadas a este cliente se llevarán a cabo perfectamente si los tokens no han expirado todavía.

Eliminación de un cliente API

1. Inicie sesión en el portal de gestión.
2. Haga clic en **Ajustes** > **Clientes API**.
3. En la lista, busque el cliente que necesite.
4. Haga clic en y en **Eliminar**.
5. Confirme su decisión.

   Todos los tokens de seguridad asignados a este cliente expirarán inmediatamente y fallarán las solicitudes a la API con estos clientes.

Importante
No hay manera de recuperar un cliente eliminado.

Referencias de integración

En la siguiente tabla se enumeran las integraciones implementadas con terceros y se muestran los enlaces a la documentación correspondiente.

NOMBRE DE LA INTEGRACIÓN	Ver en línea	Abrir PDF
Autotask PSA	https://www.acronis.com/support/documentation/AutotaskPSA/	https://dl.acronis.com/u/pdf/AutotaskPSA_Integration_quickstartguide_en-US.pdf
CloudBlue Commerce	https://www.acronis.com/support/documentation/CloudBlueCommerce/	https://dl.acronis.com/u/pdf/CloudBlue_Commerce_Integration_Guide_en-US.pdf
CloudBlue PSA	https://www.acronis.com/support/documentation/CloudBluePSA/	https://dl.acronis.com/u/pdf/CloudBluePSAIntegration_quickstartguide_en-US.pdf
ConnectWise Automate	https://www.acronis.com/support/documentation/ConnectWiseAutomate/	https://dl.acronis.com/u/pdf/AcronisConnectWiseAutomatePlugin_userguide_en-US.pdf

NOMBRE DE LA INTEGRACIÓN	Ver en línea	Abrir PDF
ConnectWise Command	https://www.acronis.com/support/documentation/ConnectWiseCommand/	https://dl.acronis.com/u/pdf/ConnectWiseCommandIntegration_quickstartguide_en-US.pdf
ConnectWise Control	https://www.acronis.com/support/documentation/ConnectWiseControl/	https://dl.acronis.com/u/pdf/ConnectWiseControl_integration_en-US.pdf
ConnectWise Manage	https://www.acronis.com/support/documentation/ConnectWiseManage/	https://dl.acronis.com/u/pdf/ConnectWiseManageIntegration_quickstartguide_en-US.pdf
Datto RMM	https://www.acronis.com/support/documentation/DattoRMM/	https://dl.acronis.com/u/pdf/DattoRMMIntegration_quickstartguide_en-US.pdf
Jamf Pro	https://www.acronis.com/support/documentation/JamfPro/	https://dl.acronis.com/u/pdf/JamfProIntegration_quickstartguide_en-US.pdf
Kaseya BMS	https://www.acronis.com/support/documentation/KaseyaBMS/	https://dl.acronis.com/u/pdf/AcronisKaseyaBMSPlugin_userguide_en-US.pdf
Kaseya VSA	https://www.acronis.com/support/documentation/KaseyaVSA/	https://download.acronis.com/pdf/AcronisKaseyaVSAPlugin_userguide_en-US.pdf
Matrix42	https://www.acronis.com/support/documentation/Matrix42/	https://dl.acronis.com/u/pdf/Matrix42Integration_quickstartguide_en-US.pdf
Microsoft Intune	https://www.acronis.com/support/documentation/MicrosoftIntune/	https://dl.acronis.com/u/pdf/MicrosoftIntuneIntegration_quickstartguide_en-US.pdf
N-able N-central	https://www.acronis.com/support/documentation/NableNcentral/	https://dl.acronis.com/u/pdf/N-able_N-central_Integration_Guide_en-US.pdf
N-able N-sight RMM	https://www.acronis.com/en-us/support/documentation/NableNsightRMM/	https://dl.acronis.com/u/pdf/N-ableN-sightRMMIntegration_quickstartguide_en-US.pdf
Ninja One	https://www.acronis.com/support/documentation/NinjaOne/	https://dl.acronis.com/u/pdf/NinjaOneIntegration_quickstartguide_en-US.pdf
Omnivoice	https://www.acronis.com/support/documentation/Omnivoice/	https://dl.acronis.com/u/pdf/OmnivoiceIntegration_quickstartguide_en-US.pdf
Plesk	https://www.acronis.com/support/documentation/Plesk/	https://dl.acronis.com/u/pdf/Acronis_Backup_extension_for_Plesk_en-US.pdf

NOMBRE DE LA INTEGRACIÓN	Ver en línea	Abrir PDF
PRTG	https://www.acronis.com/support/documentation/PRTG/	https://dl.acronis.com/u/pdf/AcronisPRTGPlugin_userguide_en-US.pdf
ServiceNow	https://www.acronis.com/support/documentation/ServiceNow/	https://dl.acronis.com/u/pdf/ServiceNow_Integration_quickstartguide_en-US.pdf
Splashtop	https://www.acronis.com/support/documentation/Splashtop/	https://dl.acronis.com/u/pdf/Splashtop_Integration_quickstartguide_en-US.pdf
TigerpawOne	https://www.acronis.com/en-us/support/documentation/TigerpawOne/	https://dl.acronis.com/u/pdf/TigerpawOneIntegration_quickstartguide_en-US.pdf
WHM & cPanel	https://www.acronis.com/en-us/support/documentation/WHMCPanel/	https://www.acronis.com/en-us/support/documentation/WHMCPanel/
WHMCS	https://www.acronis.com/en-us/support/documentation/WHMCS/	https://dl.acronis.com/u/pdf/WHMCS_Integration_Manual_en-US.pdf

Integración con VMware Cloud Director

Un proveedor de servicios puede integrar VMware Cloud Director (antes VMware vCloud Director) con Cyber Protect Cloud y ofrecer a sus clientes una solución de copia de seguridad para sus máquinas virtuales que no precisa instalación.

La integración incluye los siguientes pasos:

1. Configuración del agente de mensajes de RabbitMQ para el entorno de VMware Cloud Director.
   RabbitMQ permite sincronizar los cambios en el entorno de VMware Cloud Director para Cyber Protect Cloud.
2. Instalación del complemento para VMware Cloud Director.
   Este complemento añade Cyber Protection a la interfaz del usuario VMware Cloud Director.
3. Implementación de un agente de gestión.
   El agente de gestión asigna automáticamente organizaciones VMware Cloud Director a clientes inquilinos en Cyber Protect Cloud y administradores de organizaciones a administradores del inquilino de cliente. Para obtener más información acerca de las organizaciones, consulte Creación de una organización en VMware Cloud Director en la base de conocimientos de VMware.
   Los inquilinos de cliente se crean en el inquilino de socio para el que está configurada la integración de VMware Cloud Director. Estos nuevos inquilinos de cliente están en el modo **Bloqueado** y los administradores de socios no pueden gestionarlos en Cyber Protect Cloud.

Nota
Solo se asignan a Cyber Protect Cloud administradores de organizaciones con direcciones de correo electrónico exclusivas en VMware Cloud Director.

4. Implementación de uno o más agentes de copia de seguridad.
   El agente de copia de seguridad proporciona funcionalidades de copia de seguridad y recuperación para las máquinas virtuales en el entorno de VMware Cloud Director.

Para deshabilitar la integración entre VMware Cloud Director y Cyber Protect Cloud, póngase en contacto con el soporte técnico.

Limitaciones

- La integración con VMware Cloud Director solo es posible para inquilinos de socios en el modo de gestión **Gestionado por el proveedor de servicio**, cuyo inquilino principal (si lo hay) también utiliza el modo de gestión **Gestionado por el proveedor de servicio**. Para obtener más información acerca de los tipos de inquilino y su modo de gestión, consulte "Creación de un inquilino" (p. 35).
  Todos los socios directos existentes pueden configurar la integración con VMware Cloud Director. Los administradores de partner pueden habilitar esta opción también para los subinquilinos mediante la selección de la casilla de verificación **Infraestructura de VMware Cloud Director propiedad de partner** al crear un inquilino de socio secundario.
- La autenticación de doble factor debe estar deshabilitada para el inquilino de socio cuya integración con VMware Cloud Director esté configurada.
- Un administrador con el rol de administrador de organización en varias organizaciones de VMware Cloud Director solo puede gestionar la copia de seguridad y la recuperación para un inquilino cliente en Cyber Protection.
- La consola web de Cyber Protection se abre en una nueva pestaña.

Requerimientos de software

Versiones de VMware Cloud Director compatibles

- VMware Cloud Director 10.0, 10.1, 10.2, 10.3, 10.4, 10.4.1

Navegadores web compatibles

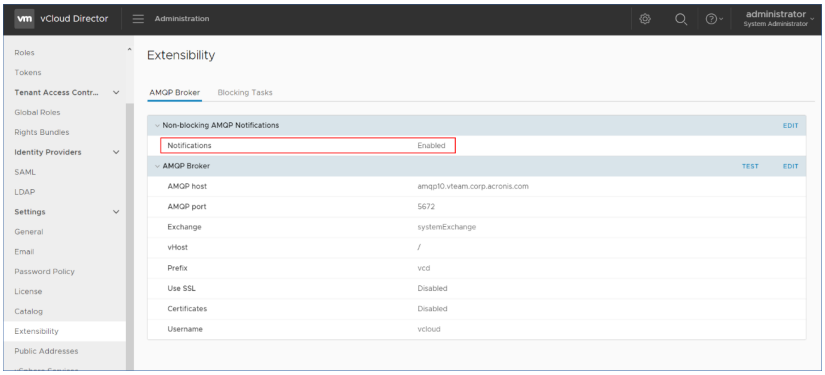
- Google Chrome 29 o posterior
- Mozilla Firefox 23 o posterior
- Opera 16 o posterior
- Microsoft Edge 25 o posterior
- Safari 8 o una versión posterior que se ejecute en los sistemas operativos macOS y iOS

En otros navegadores web (incluido Safari para otros sistemas operativos), es posible que la interfaz de usuario no se muestre correctamente o que algunas funciones no estén disponibles.

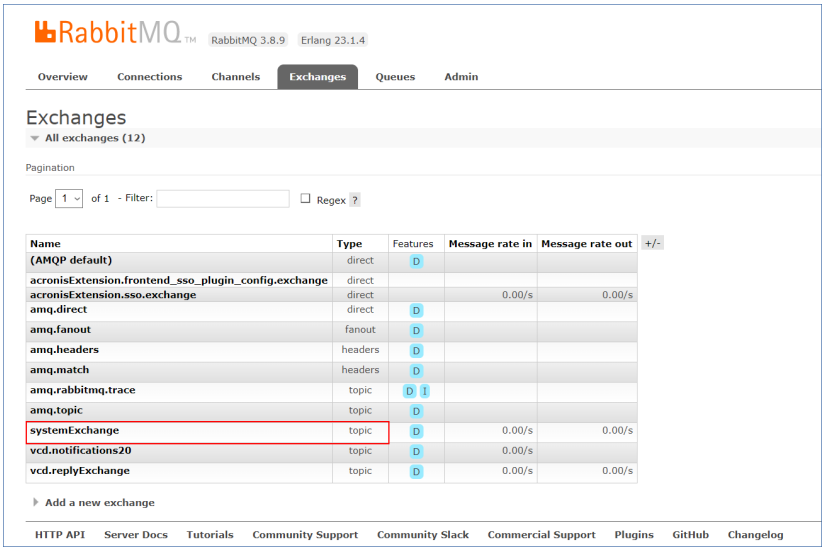
Configuración del agente de mensajes de RabbitMQ

1. Instale un agente AMQP de RabbitMQ para su entorno VMware Cloud Director.

   Para obtener más información sobre cómo instalar RabbitMQ, consulte la documentación de VMware: Instalar y configurar un agente AMQP de RabbitMQ.
2. Inicie sesión en el portal del proveedor VMware Cloud Director como administrador del sistema.
3. Vaya a **Administración** > **Extensibilidad**, y compruebe que las **Notificaciones** de **Notificaciones de AMQP sin bloqueo** están habilitadas.



4. Inicie sesión como administrador en la consola de gestión de RabbitMQ.
5. En la pestaña **Intercambios**, compruebe que se ha creado el intercambio (de forma predeterminada, con el nombre **SystemExchange**) y que su tipo es **tema**.



Instalación del complemento para VMware Cloud Director

1. Haga clic en el siguiente enlace para descargar el archivo **vCDPlugin.zip**: https://dl.managed-protection.com/u/vCD/vCDPlugin.zip.
2. Inicie sesión en el portal del proveedor VMware Cloud Director como administrador del sistema.

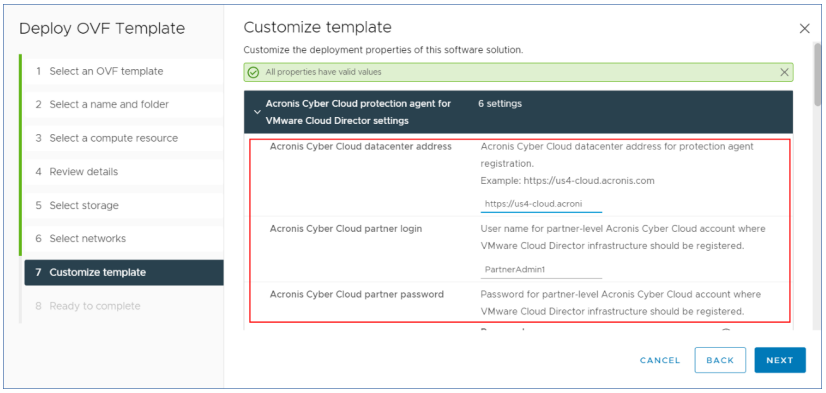
3. En el menú navegación, seleccione **Personalizar portal**.
4. En la pestaña **Gestionar complementos**, haga clic en **Cargar**.

   Se abre el asistente para **Cargar complemento**.
5. Haga clic en **Seleccionar archivo de complemento** y, a continuación, seleccione el archivo **vCDPlugin.zip**.
6. Haga clic en **Siguiente**.
7. Configure el alcance y la publicación:
   a. En la sección **Ámbito para**, seleccione solo la casilla de verificación **Inquilinos**.
   b. En la sección **Publicar para**, seleccione **Todos los inquilinos** para habilitar el complemento para todos los inquilinos existentes y futuros o seleccione los inquilinos individuales para los que desea habilitar el complemento.
8. Haga clic en **Siguiente**.
9. Revise los ajustes y, a continuación, haga clic en **Finalizar**.

Instalación de un agente de gestión

1. Inicie sesión en el portal de gestión de Cyber Protect Cloud como administrador de socios.
2. Vaya a **Configuración** > **Ubicación** y haga clic en **AñadirVMware Cloud Director**.
3. Haga clic en el enlace **Agente de gestión** y descargue el archivo ZIP.
4. Extraiga el archivo de la plantilla del agente de gestión `vCDManagementAgent.ovf` y el archivo del disco duro virtual `vCDManagementAgent-disk1.vmdk`.
5. En vSphere Client, implemente la plantilla OVF del agente de gestión en un host ESXi con una instancia de vCenter gestionada por VMware Cloud Director.

   Importante
   Instale solo un agente de gestión por entorno de VMware Cloud Director.
6. En el asistente para **implementar la plantilla OVF**, configure el agente de gestión de la siguiente forma:



   a. URL del centro de datos Cyber Protect Cloud. Por ejemplo, `https://us5-cloud.example.com`.
   b. Inicio de sesión del administrador de socios y contraseña.

c. ID del almacenamiento de la copia de seguridad para máquinas virtuales en el entorno VMware Cloud Director. Este almacenamiento de copia de seguridad solo puede ser propiedad de un partner. Para obtener más información acerca de los almacenamientos, consulte "Gestión de ubicaciones y almacenamiento" (p. 70).

   Para comprobar el ID, en el portal de gestión, vaya a **Configuración** > **Ubicaciones**, y seleccione el almacenamiento deseado. Puede ver su ID después de la parte **uuid=** de la URL.

d. Modo de facturación de Cyber Protect Cloud: **Por gigabyte** o **Por carga de trabajo**.

   Nota
   El modo de facturación seleccionado se aplica a todos los nuevos inquilinos de cliente que se creen.

e. Parámetros VMware Cloud Director: dirección de la infraestructura, inicio de sesión del administrador del sistema y contraseña.

f. Parámetros de RabbitMQ: dirección del servidor, puerto, nombre del servidor virtual, inicio de sesión del administrador y contraseña.

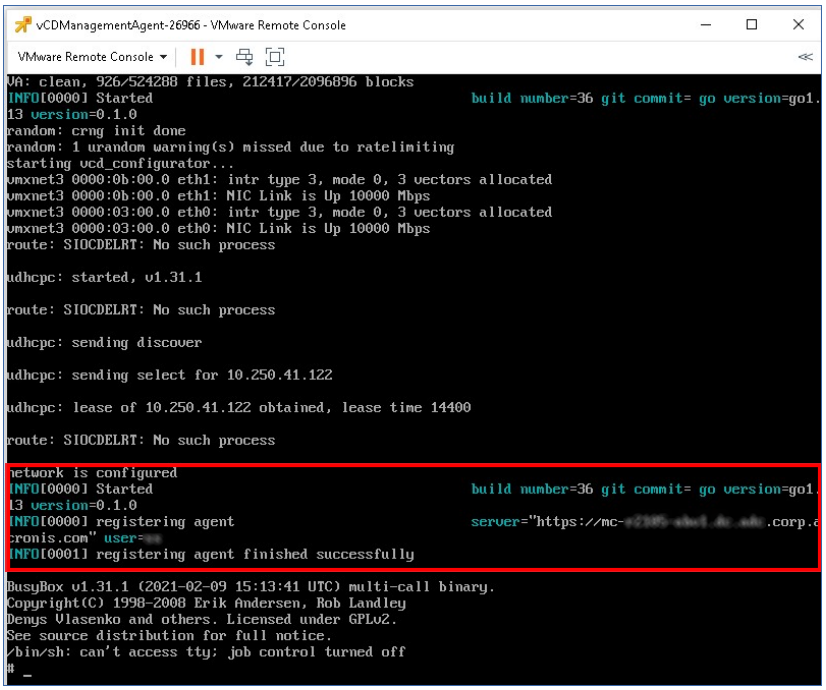
g. Parámetros de red: Dirección IP, máscara de subred, puerta de enlace predeterminada, DNS, sufijo DNS.

   De forma predeterminada, solo se habilita una interfaz de red. Para habilitar una segunda interfaz de red, seleccione la casilla de verificación junto a **Habilitar eth1**.

   Nota
   Asegúrese de que su configuración de red permita que el agente de gestión acceda tanto al entorno de VMware Cloud Director como a su centro de datos Cyber Protect Cloud.

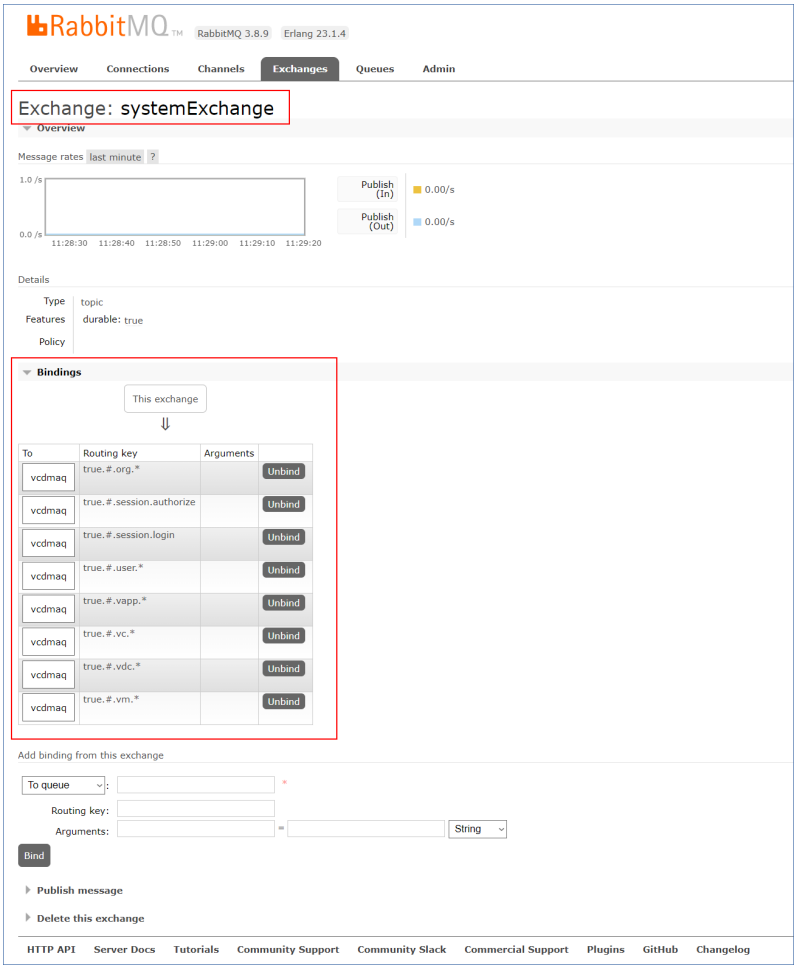
También puede configurar el agente de gestión después del despliegue inicial. En vSphere Client, desconecte la máquina virtual del agente de gestión y haga clic en **Configurar** > **Configuración** > **Opciones de vApp**. Aplique la configuración deseada y conecte la máquina virtual al agente de gestión.

7. [Opcional] En vSphere Client, abra la consola de la máquina virtual con el agente de gestión y compruebe su instalación.



8. Verifique la conexión a RabbitMQ.
   a. Inicie sesión como administrador en la consola de gestión de RabbitMQ.
   b. En la pestaña **Intercambios**, seleccione el intercambio que estableció durante la instalación de RabbitMQ. De forma predeterminada, su nombre es **systemExchange**.

c. Verifique los enlaces a la cola **vcdmaq**.



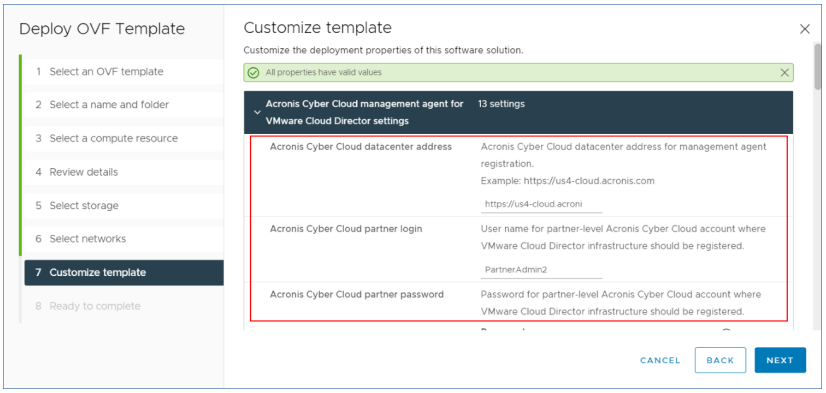
Instalación de agentes de copia de seguridad

1. Inicie sesión en el portal de gestión como administrador de socios.
2. Vaya a **Configuración** > **Ubicación** y haga clic en **AñadirVMware Cloud Director**.
3. Haga clic en el enlace **Agente de copia de seguridad** y descargue el archivo ZIP.
4. Extraiga el archivo de la plantilla del agente de copia de seguridad `vCDCyberProtectAgent.ovf` y el archivo del disco duro virtual `vCDCyberProtectAgent-disk1.vmdk`.
5. En vSphere Client, implemente la plantilla del agente de copia de seguridad al servidor ESXi que desee.

   Necesita al menos un agente de copia de seguridad por host. De forma predeterminada, se asignan al agente de copia de seguridad 8 GB de RAM y 2 CPU y pueden procesar hasta 10 tareas de copia de seguridad o recuperación simultáneamente. Para procesar más tareas o distribuir la copia de seguridad y el tráfico de recuperación, implemente agentes adicionales en el mismo host.

Nota
Las copias de seguridad de las máquinas virtuales de los host ESXi que no tienen instalado un agente de copia de seguridad fallarán con el error "Tiempo de espera de la tarea agotado".

6. En el asistente para **implementar la plantilla OVF**, configure el agente de copia de seguridad de la siguiente forma:



a. URL del centro de datos Cyber Protect Cloud. Por ejemplo, `https://us5-cloud.example.com`.

b. Inicio de sesión del administrador de socios y contraseña.

c. Parámetros de VMware vCenter: dirección del servidor, inicio de sesión y contraseña.

   El agente utilizará estas credenciales para conectase a vCenter Server. Le recomendamos utilizar una cuenta asignada al rol de **Administrador**. Si no, proporcione una cuenta con los privilegios necesarios en el servidor vCenter Server.

d. Parámetros de red: Dirección IP, máscara de subred, puerta de enlace predeterminada, DNS, sufijo DNS.

   De forma predeterminada, solo se habilita una interfaz de red. Para habilitar una segunda interfaz de red, seleccione la casilla de verificación junto a **Habilitar eth1**.

   Nota
   Asegúrese de que su configuración de red permitirá que el agente de copia de seguridad acceda tanto a vCenter Server como a su centro de datos Cyber Protect Cloud.

e. Límite de descarga: la tasa de velocidad máxima de descarga (en Kbps), que define la velocidad de lectura del archivo de copia de seguridad durante la operación de recuperación. El valor predeterminado es 0: ilimitado.

f. Límite de carga: la tasa de velocidad máxima de carga (en Kbps), que define la velocidad de escritura del archivo de copia de seguridad durante la operación de copia de seguridad. El valor predeterminado es 0: ilimitado.

También puede configurar los parámetros de configuración del agente de copia de seguridad después del despliegue inicial. En vSphere Client, desconecte la máquina virtual del agente de copia de seguridad y haga clic en **Configurar** > **Configuración** > **Opciones de vApp**. Aplique la configuración deseada y conecte la máquina virtual al agente de copia de seguridad.

7. En vSphere Client, asegúrese de que el **Servidor** y **Storage vMotion** están deshabilitados para la máquina virtual con el agente de copia de seguridad.

Actualización de agentes

Para actualizar un agente de gestión

1. Inicie sesión en el portal de gestión de Cyber Protect Cloud como administrador de socios.
2. Vaya a **Configuración** > **Ubicación** y haga clic en **AñadirVMware Cloud Director**.
3. Haga clic en el enlace **Agente de gestión** y, a continuación, descargue el archivo ZIP con el agente más reciente.
4. Extraiga el archivo de la plantilla del agente de gestión `vCDManagementAgent.ovf` y el archivo del disco duro virtual `vCDManagementAgent-disk1.vmdk`.
5. En vSphere Client, desconecte la máquina virtual del agente de gestión actual.
6. Implemente una máquina virtual con el nuevo agente de gestión mediante los archivos más recientes `vCDManagementAgent.ovf` y `vCDManagementAgent-disk1.vmdk`.
7. Configure el agente de gestión con los mismos ajustes que el antiguo.
8. [Opcional] Elimine la máquina virtual con el antiguo agente de gestión.

Importante
Solo debe tener un agente de gestión activo por entorno de VMware Cloud Director.

Para actualizar un agente de copia de seguridad

1. Inicie sesión en el portal de gestión de Cyber Protect Cloud como administrador de socios.
2. Vaya a **Configuración** > **Ubicación** y haga clic en **AñadirVMware Cloud Director**.
3. Haga clic en el enlace **Agente de copia de seguridad** y descargue el archivo ZIP con el agente más reciente.
4. Extraiga el archivo de la plantilla del agente de gestión `vCDCyberProtectAgent.ovf` y el archivo del disco duro virtual `vCDCyberProtectAgent-disk1.vmdk`.
5. En vSphere Client, desconecte la máquina virtual del agente de copia de seguridad actual.
   Todas las tareas de copia de seguridad y recuperación que puedan estar ejecutándose fallarán. Para comprobar si se están ejecutando tareas, en vSphere Client, abra la consola de la máquina virtual con el agente de copia de seguridad y, a continuación, ejecute el comando `ps | grep esx_worker`. Compruebe que no hay procesos `esx_worker` activos.
6. Implemente una máquina virtual con el nuevo agente de copia de seguridad mediante los archivos más recientes `vCDCyberProtectAgent.ovf` y `vCDCyberProtectAgent-disk1.vmdk`.
7. Configure el agente de copia de seguridad con los mismos ajustes que el antiguo.
8. [Opcional] Elimine la máquina virtual con el antiguo agente de copia de seguridad.

Acceso a la consola web de Cyber Protection

Los siguientes administradores pueden gestionar la copia de seguridad de equipos virtuales en las organizaciones de VMware Cloud Director:

- Administradores de la organización
- Administradores de copias de seguridad asignados específicamente
  Para obtener más información sobre cómo crear dicho administrador, consulte "Crear un administrador de copias de seguridad" (p. 154).

Los administradores pueden acceder a la consola web de Cyber Protection personalizada al hacer clic en **Ciberprotección** en el menú de navegación del portal del inquilino VMware Cloud Director.

Nota
El inicio de sesión único está disponible solo para los administradores de la organización y no para los administradores del sistema que utilizan el portal del inquilino VMware Cloud Director.

En la consola web de Cyber Protection, los administradores solo pueden acceder a sus propios elementos de la organización VMware Cloud Director: centros de datos virtuales, vapulas y máquinas virtuales individuales. Pueden gestionar la copia de seguridad y la recuperación de los recursos de la organización VMware Cloud Director.

Los administradores de socios pueden acceder a las consolas web de Cyber Protection de sus inquilinos de cliente y pueden gestionar la copia de seguridad y la recuperación en su nombre.

Limitaciones

La lista de limitaciones está sujeta a cambios en los próximos lanzamientos de Cyber Protect Cloud.

Copia de seguridad

- Solo se admite la copia de seguridad del equipo al completo. No están permitidos los filtros de archivo ni seleccionar discos o volúmenes.
- Solo se admite el almacenamiento en la nube como ubicación de la copia de seguridad. El almacenamiento se configura en los ajustes del agente de gestión y los usuarios no pueden cambiarlo en el plan de protección.
- No se admiten grupos dinámicos.
- Los siguientes esquemas de copias de seguridad son compatibles: **Siempre incremental (un solo archivo)**, **Siempre completas** y **Completas semanalmente, incrementales diariamente**.
- Solo es compatible la limpieza después de la copia de seguridad.

Recuperación

- Solo es compatible la recuperación en la máquina virtual original. La máquina virtual original debe existir en el entorno VMware Cloud Director.
- La recuperación a nivel de archivo no se admite.

Crear un administrador de copias de seguridad

Los administradores de organización pueden delegar la gestión de copias de seguridad en administradores de copias de seguridad asignados específicamente.

Pasos para crear un administrador de copias de seguridad

1. En el portal inquilino VMware Cloud Director, haga clic en **Administración** > **Roles** > **Nuevo**.
2. En la ventana **Añadir rol**, especifique un nombre y una descripción para el nuevo rol.
3. Desplace hacia abajo la lista de permisos y, a continuación, en **Otro**, seleccione **Operador de copias de seguridad de máquina virtual de autoservicio**.

   Nota
   El permiso **Operador de copias de seguridad de máquina virtual de autoservicio** estará disponible después de instalar el complemento para VMware Cloud Director. Para obtener más información sobre cómo hacerlo, consulte "Instalación del complemento para VMware Cloud Director" (p. 146).

4. En el portal inquilino VMware Cloud Director, haga clic en **Usuarios**.
5. Seleccione un usuario y haga clic en **Editar**.
6. Asigne a este usuario el nuevo rol que ha creado.

Como resultado, el usuario seleccionado podrá gestionar las copias de seguridad de las máquinas virtuales de esta organización.

Nota
Los administradores de sistemas del entorno de VMware Cloud Director pueden definir un rol global con el permiso **Operador de copias de seguridad de máquina virtual de autoservicio** activado y publicar este rol en los inquilinos. De este modo, los administradores de la organización solo necesitarán asignar el rol a un usuario.

Informe del sistema, archivos de registro y archivos de configuración

Para fines de solución de problemas, puede que deba crear un informe del sistema con la herramienta `sysinfo` o comprobar los archivos de registro y de configuración de una máquina virtual con un agente.

Puede acceder a la máquina virtual tanto directamente, abriendo su consola en vSphere Client, o de forma remota, a través de un cliente SSH. Para acceder a la máquina virtual mediante un cliente SSH, primero debe habilitar la conexión SSH en ese equipo.

Para habilitar la conexión SSH en una máquina virtual

1. En vSphere Client, abra la consola de la máquina virtual con el agente.
2. En el símbolo del sistema, ejecute el siguiente comando para iniciar el daemon SSH: `/bin/sshd`.

Como resultado, podrá conectarse a esta máquina virtual mediante un cliente SSH, como WinSCP, por ejemplo.

Cómo ejecutar la herramienta `sysinfo`

1. Acceda a la máquina virtual con el agente.
   - Para acceder directamente, en vSphere Client, abra la consola de la máquina virtual.
   - Para acceder de forma remota, conéctese a la máquina virtual mediante un cliente SSH.
     Utilice el siguiente inicio de sesión predeterminado: combinación de contraseña: `root`:`root`.
2. Vaya al directorio `/bin` y, a continuación, ejecute la herramienta `sysinfo`.

   ```
   # cd /bin/
   # ./sysinfo
   ```

   Como resultado, se guardará un archivo de informe del sistema en el directorio predeterminado: `/var/lib/Acronis/sysinfo`.
   Puede especificar otro directorio ejecutando la herramienta `sysinfo` con la opción `--target_dir`.

   ```
   ./sysinfo --target_dir path/to/report/dir
   ```

3. Descargue el informe del sistema generado mediante un cliente SSH.

Para acceder a un archivo de registro o de configuración

1. Conéctese a la máquina virtual mediante un cliente SSH.
   Utilice el siguiente inicio de sesión predeterminado: combinación de contraseña: `root`:`root`.
2. Descargue el archivo que desee.
   Puede encontrar los archivos de registro en las siguientes ubicaciones:
   - Agente de copia de seguridad: `/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log`
   - Agente de gestión: `/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log`

   Puede encontrar los archivos de configuración en las siguientes ubicaciones:
   - Agente de copia de seguridad: `/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml`
   - Agente de gestión: `/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml`

Eliminación de la integración con VMware Cloud Director

Revertir la configuración y cancelar el registro de la instancia VMware Cloud Director desde Cyber Protect Cloud es un procedimiento complejo. Si necesita ayuda, póngase en contacto con su representante de soporte técnico.

Configuración de privacidad

La configuración de privacidad le ayuda a indicar si da o no su consentimiento para la recopilación, uso y divulgación de su información personal.

En función del país en el que utilice Cyber Protect y del centro de datos de Cyber Protect Cloud que le preste servicios, es posible que, al iniciar Cyber Protect por primera vez, se le pida que confirme si acepta el uso de Google Analytics en Cyber Protect.

Google Analytics nos ayuda a comprender mejor el comportamiento de los usuarios y a mejorar su experiencia en Cyber Protect mediante la recopilación de datos anónimos.

Si no ve el consentimiento y los menús de Google Analytics en la interfaz de Cyber Protect, significa que Google Analytics no se utiliza en su país.

Si ha habilitado o rechazado la habilitación de Google Analytics en el lanzamiento inicial de Cyber Protect, puede cambiar su decisión en cualquier momento.

Pasos para habilitar o deshabilitar Google Analytics

1. En la consola de Cyber Protect, haga clic en el icono de la cuenta en la esquina superior derecha.
2. Seleccione **Mi configuración de privacidad**.
3. En la sección **Recopilación de datos de Google Analytics**, haga clic en uno de los siguientes botones:
   - **Encendido** para habilitar Google Analytics
   - **Apagado** para deshabilitar Google Analytics

Índice

#

#CyberFit Score por equipo 86

¿

¿Qué es un cliente API? 139

A

Acceso a la consola de Cyber Protection desde el portal de administración 28

Acceso a la consola web de Cyber Protection 153

Acceso a los servicios 30

Acceso al portal de gestión 27

Acciones de la lista de dispositivos 70

Acerca de Cyber Protect 7

Acerca de este documento 6

Activación de la cuenta de administrador. 26

Activación de las notificaciones de mantenimiento 42

Actualización de agentes 152

Actualización de agentes automáticamente 81

Actualizaciones que faltan por categoría 97

Actualizar los datos de uso para un inquilino 46

Agregar almacenamientos nuevos 71

Alertas sobre el estado del disco 93

Ámbito del informe 103

Apariencia 76

Aplicaciones para móviles 78

Aplicar etiquetas blancas 79

Artículos de oferta 13

Artículos de oferta y gestión de cuotas 13

Asistente para la autodetección 69

B

Barra del historial de siete días 32

C

Cambiar el modo de facturación de un inquilino cliente 12

Cambiar el modo de facturación de un inquilino partner 12

Cambiar la cuota de servicio de equipos 23

Cambiar los ajustes de notificaciones para un usuario 57

Cambio desde las ediciones heredadas al modelo de licencias actual 10

Campos del registro de control 127

Características avanzadas incluidas en el servicio de protección 130

Características avanzadas y de pago por uso en el servicio de protección 134

Características y paquetes avanzados incluidos en los servicios de Cyber Protect 130

Cómo funciona 61, 90

Cómo mover a un inquilino 47

Configuración de contactos en el asistente de Perfil de empresa 27

Configuración de cuotas flexibles y estrictas 16

Configuración de documentos legales 77

Configuración de los contactos de la empresa 43

Configuración de los elementos de oferta para un inquilino 39

Configuración de los informes de uso personalizados 104

Configuración de los informes de uso planificados 104

Configuración de personalización de marca 78

Configuración de personalización de marca y etiquetado en blanco 75

Configuración de privacidad 157

Configuración de situaciones relacionadas con la venta de productos de gama superior a sus clientes 68

Configuración de una integración de Cyber Protect Cloud 139

Configuración de URL de la interfaz web personalizadas 80

Configuración del agente de mensajes de RabbitMQ 146

Configuración del almacenamiento inmutable 72

Configuración del informe resumido ejecutivo 120

Configuración del perfil del cliente administrado de forma automática 43

Configuración del servidor de correo electrónico 78

Conmutación entre ediciones y modos de facturación 10

Conversión de un inquilino socio en un inquilino carpeta y viceversa 48

Copia de seguridad 153

Creación de un cliente API 140

Creación de un inquilino 35

Creación de una cuenta de usuario 50

Crear o editar un plan de protección 69

Crear un administrador de copias de seguridad 154

Crear un informe resumido ejecutivo 120

Cuotas de almacenamiento 19

Cuotas de Backup 17

Cuotas de certificación 22

Cuotas de Disaster Recovery 21

Cuotas de envío de datos físicos 22

Cuotas de File Sync & Share 22

Cuotas de orígenes de datos en el cloud 17

Cuotas flexibles y rígidas 15

D

Datos informados según el tipo de widget 124

Dependencia de instalador de agente para artículos de oferta 24

Descargar datos de cargas de trabajo afectadas recientemente 99

Descargar un informe 109

Deshabilitación de un cliente API 141

Deshabilitación y habilitación de un inquilino 46

Deshabilitación y habilitación de una cuenta de usuario 59

Deshabilitar la personalización de marca 79

Detalles del análisis de copias de seguridad 98

Distribución de los principales incidentes por carga de trabajo 87

Documentación y soporte técnico 77

E

Edición de la configuración de informes 107

Ejemplo

de la edición de Cyber Protect por carga de trabajo al modo de facturación por carga de trabajo 11

Pasos para cambiar de una edición Advanced de Cyber Protect a una facturación por carga de trabajo 11

Elementos afectados recientemente 98

Elementos de personalización de marca 76

Eliminación de almacenamientos 72

Eliminación de la integración con VMware Cloud Director 156

Eliminación de un cliente API 142

Eliminación de un inquilino 49

Eliminación de una cuenta de usuario 60

Enviar informes resumidos ejecutivos 122

Equipos detectados 85

Equipos vulnerables 95

Establecimiento de la autenticación de doble factor 61

Establecimiento de la autenticación de doble factor para el inquilino 64

Estado de instalación del parche 96

Estado de la protección 85

Estado de la red de las cargas de trabajo 89

Exportación e importación de la estructura del informe 109

F

Facturación de certificación 9

Facturación del envío de datos físicos 9

Filtrado y búsqueda 128

Funciones de usuario disponibles para cada servicio 52

G

Generación de informes 102

Gestión de almacenamiento 71

Gestión de clientes API 139

Gestión de inquilinos 35

Gestión de la autenticación de doble factor para usuarios 65

Gestión de ubicaciones y almacenamiento 70

Gestión de usuarios 50

Gráfico de quemado de incidentes de seguridad 88

H

Habilitación de servicios para varios inquilinos existentes 40

Habilitación de un cliente API deshabilitado 141

Habilitar la prevención avanzada de la pérdida de datos 135

Habilitar o deshabilitar artículos de oferta 14

Habilitar Seguridad avanzada + EDR 136

Historial de instalación de parches 97

Historial de sesión 102

I

Impedir que los usuarios de Microsoft 365 sin licencia inicien sesión 20

Incorporación de un informe 107

Informe del sistema, archivos de registro y archivos de configuración 154

Informes de operaciones 105

Instalación de agentes de copia de seguridad 150

Instalación de un agente de gestión 147

Instalación del complemento para VMware Cloud Director 146

Integración con sistemas externos 139

Integración con VMware Cloud Director 144

Integraciones 139

L

Las cuentas de usuario y los inquilinos 33

Limitación del acceso a la interfaz web 29

Limitación del acceso a su inquilino 48

Limitaciones 38, 89, 145, 153

Lista de vulnerabilidades 69

M

Mapa de protección de datos 93

Marcas blancas 79

Modo Seguridad aumentada 38

Modos de facturación del componente Protección 8

Modos de facturación para Cyber Protect 8

Modos de facturación para File Sync & Share 9

Modos de facturación y ediciones 14

Mover un inquilino a otro inquilino 46

N

Navegación en el portal de gestión 29

Navegadores web compatibles 26, 145

Niveles en los que se pueden definir las cuotas 16

Notificaciones recibidas por cada función de usuario 59

O

Operaciones 83

Operaciones con ubicaciones 71

P

Paquetes Advanced Protection 129

Para deshabilitar la autenticación de doble factor para el inquilino 65

Para deshabilitar la autenticación de doble factor para un usuario 66

Para habilitar la autenticación de doble factor para el inquilino 64

Para habilitar la autenticación de doble factor para un usuario 67

Para restablecer los navegadores de doble confianza para un usuario 66

Parámetros con uso cero 103

Pasos para actualizar agentes automáticamente 81

Pasos para gestionar los servicios para un inquilino 39

Pasos para restablecer la autenticación de doble factor para un usuario 65

Pasos para supervisar las actualizaciones de los agentes 83

Personalización de marca del agente y el programa de instalación 76

Personalizar un informe resumido ejecutivo 121

Pestaña Clientes 31

Pestaña General 30

Prevención avanzada de la pérdida de datos 135

Proceso de integración habitual 140

Programación de un informe 108

Propagación de la configuración de doble factor en niveles de inquilino 62

Protección de correo electrónico avanzada 138

Protección de fuerza bruta 67

Puntos de venta de productos de gama superior que se muestran a un cliente 69

R

Rebasamiento de la cuota de almacenamiento de copias de seguridad 19

Recuperación 154

Recuperación ante desastres avanzada 137

Referencias de integración 142

Registro de control 126

Requerimientos de software 145

Requisitos de contraseña 26

Requisitos y restricciones 47

Restablecimiento de la autenticación de doble factor en caso de pérdida de dispositivo de segundo factor 67

Restablecimiento del valor secreto de un cliente API 141

Restaurar la configuración predeterminada de personalización de marca. 79

Resumen de la instalación del parche 97

Resumen ejecutivo 109

Roles de usuario y derechos de la Programación cibernética 55

S

Seguridad avanzada + EDR 136

Selección de ubicaciones y almacenamientos para socios y clientes 70

Servicios 13

Servicios de Cyber Protect 7

Servicios y elementos de oferta 13

Supervisión 65, 83

Supervisión del estado del disco 89

T

Tiempo medio de reparación de incidentes 87

Tipo de informe 103

Tipo de inquilinos que se pueden mover 47

Transferencia de la propiedad de una cuenta de usuario 60

Transformación de la cuota de copia de seguridad 20

U

Ubicaciones 70

URL bloqueadas 99

URL para los servicios de Cyber Protect Cloud 77

Uso 83, 102

Uso de los modelos de facturación con ediciones heredadas 9

Uso del portal de gestión 26

V

Venta de productos de gama superior 78

Versiones de VMware Cloud Director compatibles 145

Volcado de los datos del informe 109

Vulnerabilidades existentes 96

W

Widget para la prevención de pérdida de datos 118

Widgets de certificación 119

Widgets de copias de seguridad 115

Widgets de Detección y respuesta de endpoints (EDR) 87

Widgets de evaluación de vulnerabilidades 95

Widgets de evaluación de vulnerabilidades y gestión de parches 116

Widgets de File Sync & Share 118

Widgets de instalación de parches 96

Widgets de inventario de hardware 101

Widgets de inventario de software 100

Widgets de protección contra malware 113

Widgets de recuperación ante desastres 116

Widgets de resumen de cargas de trabajo 110

Widgets de resúmenes ejecutivos 110

Widgets sobre el estado del disco 90

Z

Zonas horarias de los informes 123