SOPHOS

Security made simple.

Sophos Enterprise Console
Guía de usuario de auditoría

Versión: 5.5

Contenido

1 Acerca de esta guía

En esta guía se describe cómo utilizar la función de auditoría de Sophos Enterprise Console para supervisar los cambios en la configuración de Enterprise Console y otras acciones del usuario y del sistema. Esta guía está dirigida al administrador de sistemas o al administrador de bases de datos.

Se asume que ya conoce y utiliza Sophos Enterprise Console (SEC).

La documentación de Sophos se encuentra en http://www.sophos.com/es-es/support/documentation.

2 Acerca de Sophos Auditing

La auditoría permite monitorizar los cambios de configuración en Enterprise Console y otras acciones del usuario y del sistema. Puede utilizar esta información para el cumplimiento normativo y la solución de problemas, o como evidencia legar en caso de actividad maliciosa.

Por defecto, la auditoría está desactivada. Una vez activada en Enterprise Console, la base de datos recogerá una entrada del tipo SophosSecurity cada vez que cambien ciertas opciones de configuración o se realicen ciertas acciones.

La entrada de auditoría incluye la siguiente información:

- Acción realizada
- Usuario que realizó la acción
- Equipo
- Subentorno del usuario
- Fecha y hora de la acción

Se registran tanto las acciones completadas como los intentos fallidos.

Puede utilizar aplicaciones de terceros, como Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services o Crystal Reports, para acceder y analizar las entradas de auditoría en la base de datos.

Importante: Sophos Auditing permite utilizar los datos en aplicaciones de terceros. Al utilizar esta función, debe asumir la responsabilidad de proteger los datos mencionados, incluyendo el uso de dichos datos por usuarios autorizados. Para conocer los aspectos relativos a la seguridad, consulte Verificar la seguridad de la base de datos en la página 6.

Para obtener más información sobre qué acciones se auditan, consulte Acciones en la auditoría en la página 21.

3 Pasos clave para utilizar Sophos Auditing

Los pasos clave para utilizar Sophos Auditing son:

- Verificar la seguridad de la base de datos
- Activar la auditoría
- Conceder acceso a los datos de auditoría
- Crear un informe de auditoría

4 Verificar la seguridad de la base de datos

4.1 Protección de la base de datos

Enterprise Console y la base de datos SophosSecurity integran diferentes funciones para la protección de los datos:

- Control de acceso
- Protección contra manipulaciones

Control de acceso

El control de acceso se aplica a las siguientes áreas:

- Interfaz de usuario

  Sólo los usuarios con permiso de **Auditoría** en Enterprise Console y que pertenecen al grupo Sophos Console Administrators pueden activar o desactivar la auditoría.

- Base de datos

  Por defecto, sólo los usuarios del grupo Sophos DB Admins tienen acceso a la base de datos. Además, se requiere un token de sesión válido para ver los procedimientos almacenados de la base de datos. El token se genera cuando el usuario accede a la interfaz gráfica o modifica el subentorno.

Protección contra manipulaciones

La base de datos está diseñada para prevenir cambios en los datos de auditoría. El contenido de la base de datos de auditoría no tiene por qué modificarse, aparte de ciertas opciones de configuración. Un sistema de seguridad evita intentos de modificar o borrar el contenido de las tablas.

Los datos sólo se pueden borrar al purgar la base de datos. Los datos con más de dos años de antigüedad se borran de forma automática. También puede utilizar la herramienta PurgeDB para purgar los datos (consulte http://www.sophos.com/es-es/support/knowledgebase/109884.aspx).

4.2 Mejorar la seguridad de la base de datos

Audite la base de datos

Además de la protección integral de las bases de datos de Enterprise Console, se recomienda establecer un control de la instancia del servidor SQL para auditar la actividad en la base de datos SophosSecurity.

Por ejemplo, si utiliza SQL Server 2008 Enterprise Edition , puede utilizar la función SQL Server Audit. Versiones anteriores de SQL Server disponen de auditoría de inicio de sesión, de cambios y eventos.

Para más información sobre estas funciones, consulte la documentación de SQL Server. Por ejemplo:

- SQL Server Audit (motor de base de datos)
- Auditoría (motor de base de datos), SQL Server 2008 R2
- Auditoría en SQL Server 2008
- Auditoría (motor de base de datos), SQL Server 2008

Cifre la conexión a la base de datos

Se recomienda cifrar la comunicación entre los clientes y las bases de datos de Enterprise Console. Para más información, consulte la documentación de SQL Server:

- Habilitar conexiones cifradas en el motor de base de datos (Administrador de configuración de SQL Server)
- Cifrar conexiones a SQL Server 2008 R2
- Cómo habilitar el cifrado SSL para una instancia de SQL Server mediante Microsoft Management Console

Controle el acceso a las copias de seguridad de la base de datos

Imponga un control de acceso restrictivo a las copias de seguridad o copias de la base de datos. De esta forma evitará el acceso no autorizado a los archivos.

Nota: los enlaces en esta sección llevan a sitios web de terceros y se incluyen como ayuda. El contenido de estas páginas podría cambiar sin nuestro conocimiento.

5 Activar Sophos Auditing

Por defecto, la auditoría está desactivada. Para activar la auditoría:

1. En Enterprise Console, en el menú **Herramientas**, haga clic en **Gestionar auditoría**.
2. En el cuadro de diálogo **Gestión de auditoría**, seleccione la opción **Activar auditoría**.

   Nota: si la opción no se encuentra disponible, quiere decir que no dispone de permiso para gestionar la auditoría. Sólo pueden gestionar la auditoría los usuarios del grupo Sophos Console Administrators con el permiso **Auditing** en Enterprise Console. Para más información sobre los permisos y la administración delegada, consulte la *Ayuda de Sophos Enterprise Console*.

6 Conceder acceso a los datos de auditoría

Por defecto, sólo administradores de sistema tienen acceso a los datos de auditoría. Para el resto de usuarios que necesiten usar los datos, conceda acceso de forma explícita mediante el permiso "Select" en el esquema **Reports** en la base de datos SophosSecurity. Puede hacerlo con la herramienta **sqlcmd** o desde SQL Server Management Studio.

6.1 Conceder permiso a los datos de auditoría mediante la herramienta sqlcmd

Para conceder acceso a los datos de auditoría:

1. Copie el siguiente script al Bloc de notas, por ejemplo.

```
USE SophosSecurity;

DECLARE @stmt NVARCHAR(max);

DECLARE @Account VARCHAR(512)

/* Sustituya <Dominio>\<Usuario> con la cuenta a la que desea
conceder acceso. */

SET @Account = N'<Domain>\<User>'

IF NOT EXISTS( SELECT * FROM sys.server_principals WHERE name =
@Account )
BEGIN
     SET @stmt = N'CREATE LOGIN [' + @Account + N'] FROM WINDOWS';

      EXEC sp_executesql @stmt;
END;

IF NOT EXISTS( SELECT * FROM sys.database_principals WHERE name
= @Account )
BEGIN
      SET @stmt = N'CREATE USER [' + @Account + N'] FOR LOGIN ['
 + @Account + N']';
      EXEC sp_executesql @stmt;
END;

SET @stmt = N'GRANT SELECT ON SCHEMA :: [Reports] TO [' + @Account
 + N']';
EXEC sp_executesql @stmt;
GO
```

2. En la línea "SET @Account = N'<Dominio>\<Usuario>'" introduzca la cuenta a la que desea conceder acceso.

   Si los equipos se encuentra en grupo de trabajo, sustituya <Dominio> por el nombre del equipo. La cuenta (con el mismo nombre y contraseña) debe existir en cada equipo desde el que desee realizar el acceso.

3. Abra la línea de comandos.
4. Conecte a la instancia del servidor SQL. Escriba:

   ```
   sqlcmd -E -S <Server>\<instancia SQL>
   ```

   La instancia predeterminada es SOPHOS.

5. Copie el script del Bloc de notas y péguelo en la línea de comandos.
6. Pulse Intro para ejecutar el script.

   El usuario obtendrá acceso a los datos de auditoría.

7. Repita esta paso con cada usuario que requiera acceso.

6.2 Conceder acceso a los datos de auditoría mediante SQL Server Management Studio

Antes de poder conceder permiso en el esquema **Reports** la base de datos SophosSecurity a un usuario mediante SQL Server Management Studio, asegúrese de que el usuario dispone de acceso al servidor SQL y es miembro del grupo SophosSecurity.

- Si el usuario ya dispone de acceso al servidor SQL, añádalo al grupo SophosSecurity de la base de datos. En Explorador de objetos, expanda el servidor, **Bases de datos**, **SophosSecurity** y **Seguridad**. Haga clic con el botón derecho en **Usuarios** y seleccione **Nuevo usuario**. En el cuadro de diálogo **Usuario de la base de datos**, introduzca el nombre de usuario y el nombre de inicio de sesión. Haga clic en **Aceptar**.

  Para obtener más información sobre cómo crear usuarios de la base de datos, consulte http://msdn.microsoft.com/es-es/library/aa337545.aspx#SSMSProcedure.

- Si es necesario, añada un nuevo nombre de inicio de sesión SQL para el usuario y hágalo miembro del grupo SophosSecurity. En Explorador de objetos, expanda servidor el servidor y **Seguridad**. Haga clic con el botón derecho en **Inicios de sesión** y seleccione **Nuevo inicio de sesión**. En el cuadro de diálogo **Inicio de sesión**, en la página **General**, introduzca el nombre de la cuenta o del grupo. En la página **Asignación de usuarios**, seleccione **SophosSecurity**. Haga clic en **Aceptar**.

  Para obtener más información sobre cómo crear inicios de sesión de SQL Server, consulte http://msdn.microsoft.com/es-es/library/aa337562.aspx#SSMSProcedure.

Para conceder acceso a los datos de auditoría mediante SQL Server Management Studio:

1. En Explorador de objetos, expanda el servidor, **Bases de datos**, **SophosSecurity**, **Seguridad** y **Esquemas**.
2. Haga clic con el botón derecho en **Informes** y seleccione **Propiedades**.
3. En el cuadro de diálogo **Propiedades de esquemas - Informes**, en la página **Permisos**, haga clic en **Buscar**. En el cuadro de diálogo **Seleccionar usuarios o roles**, añada el usuario.
4. Para cada usuario, en la sección **Permisos de <usuario>**, en la ficha **Explícito**, haga clic en **Seleccionar** bajo **Conceder** y haga clic en **Aceptar**.

7 Crear un informe de auditoría en Microsoft Excel

En este ejemplo se muestra cómo importar datos del servidor SQL y cómo anlizarlos en Microsoft Excel 2010.

En las siguientes secciones se describe cómo crear un informe de auditoría en Microsoft Excel, incluyendo:

- Configurar la conexión a la base de datos (fuente de datos).
- Crear consultas en Microsoft Query.
- Devolver datos a Excel.
- Crear informes en Excel (tabla o tabla dinámica).

Nota: se recomienda utilizar los identificadores numéricos en vez de la cadena del valor para realizar enlaces lógicos con los datos obtenidos. Por ejemplo, en vez de usar el valor del campo **TargetType**, utilice el valor del campo **TargetTypeId**. De esta forma evitará problemas de compatibilidad con próximas ediciones de Enterprise Console. Para ver una tabla de ID numéricos, consulte Apéndice: Identificadores numéricos de los valores de campos de datos en la página 29.

Para más información sobre cómo importar datos del servidor SQL y crear informes en Excel, consulte la documentación de Microsoft.

7.1 Configurar la conexión a la base de datos

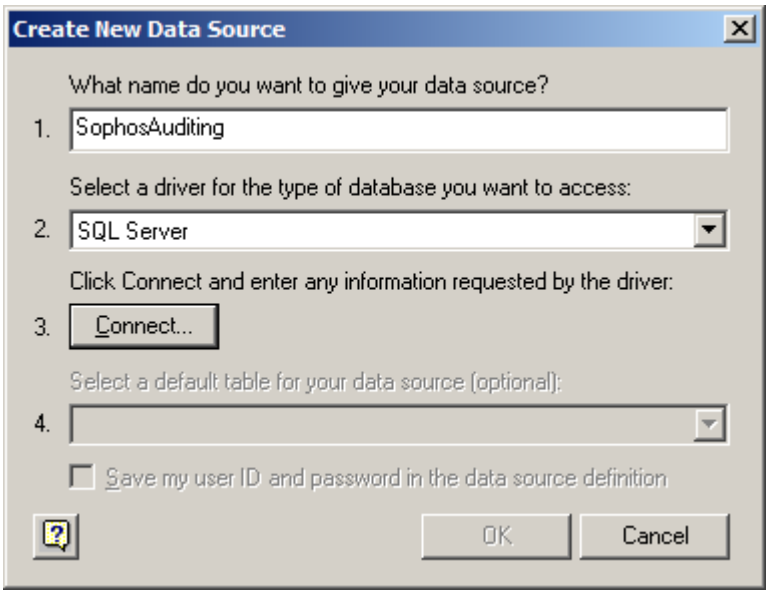
Primero debe conectar a la base de datos.

1. Abra Excel. En la ficha **Datos**, en el grupo **Obtener datos externos**, haga clic en **Desde otro origen** y seleccione **Desde Microsoft Query**.

   Se abrirá el cuadro de diálogo **Elegir origen de datos**.

2. En la ficha **Bases de datos**, deje seleccionado **<Nuevo origen de base de datos>** y haga clic en Aceptar.
3. En el cuadro de diálogo **Crear nuevo origen de datos**, escriba el nombre para la fuente de datos. En este ejemplo se utiliza el nombre **SophosAuditing**.

4. En el cuadro **Seleccione un controlador para el tipo de base de datos a la que desea obtener acceso**, seleccione **SQL Server**.

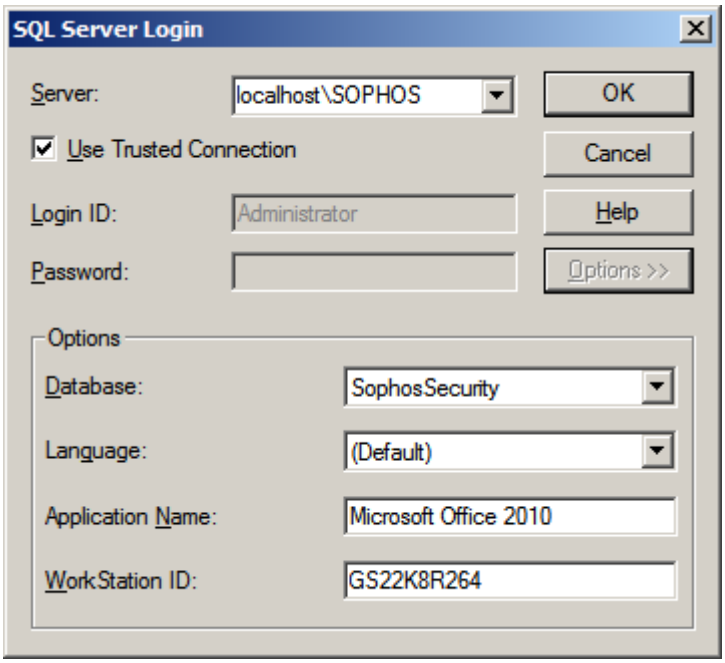


   Haga clic en **Conectar**.

5. En el cuadro de diálogo **Inicio de sesión de SQL Server**, en el cuadro **Servidor**, introduzca el nombre del servidor SQL al que desea conectar.

   En este ejemplo, la conexión se realiza a la instancia SOPHOS en ese mismo equipo (localhost).

6. Haga clic en **Opciones** para expandir el panel. En el cuadro **Base de datos**, seleccione **SophosSecurity**.



   Haga clic en **Aceptar**.

7. En el cuadro de diálogo **Crear nuevo origen de datos**, en **Seleccione una tabla predeterminada para el origen de datos (opcional)**, seleccione **vAuditEventsAll**.

   Haga clic en **Aceptar**.

7.2 Crear consultas

En este ejemplo se muestra cómo realizar una consulta a la fuente de datos que acaba de crear sobre los cambios en políticas de control de datos en los últimos tres meses.

1. En el cuadro de diálogo **Elegir origen de datos**, desactive la opción **Usar el Asistente para consultas para crear o modificar consultas**.
2. Seleccione la fuente de datos creada anteriormente (en este ejemplo, **SophosAuditing**) y haga clic en **Aceptar**.

   El cuadro de diálogo **Microsoft Query** muestra **Consulta de SophosAuditing** con la tabla predeterminada, **vAuditEventsAll**, seleccionada al crear la fuente de datos.

3. Escoja una de las siguientes opciones:
   - Crear la consulta en la vista de diseño.
     1. En el cuadro de diálogo **Microsoft Query**, en el menú **Criterio**, seleccione **Agregar criterios**.
     2. En el cuadro de diálogo **Agregar criterios**, junto a **Campo**, seleccione **Timestamp**. Deje en blanco el campo **Operador**. En el campo **Valor**, escriba:

        `>=DATEADD(mm,-3,GETUTCDATE())`

        Utilice el separador de listas especificado en la Configuración regional y de idioma del Panel de control. Por ejemplo, si el separador de listas especificado en su equipo es el punto y coma, utilice punto y coma en lugar de las comas. Puede que aparezca el error "Extra ')'" si utiliza un separador incorrecto.

        Haga clic en **Añadir**. Se añade el criterio a la **Consulta de SophosAuditing**.

     3. En el cuadro de diálogo **Agregar criterios**, junto a **Campo**, seleccione **TargetType**. En el campo **Operador**, seleccione **igual**. En el campo **Valor**, seleccione o escriba **Policy**.

        Haga clic en **Añadir**. Se añade el criterio a la **Consulta de SophosAuditing**.

     4. En el cuadro de diálogo **Agregar criterios**, junto a **Campo**, seleccione **TargetSubType**. En el campo **Operador**, seleccione **igual**. En el campo **Valor**, seleccione o escriba **Data control**.

        Haga clic en **Añadir**. Se añade el criterio a la **Consulta de SophosAuditing**.

        En el cuadro de diálogo **Agregar criterios**, haga clic en **Cerrar**.

     5. En el cuadro de diálogo **Microsoft Query**, añada los campos de **vAuditEventsAll** a la consulta. Puede hacer doble clic o arrastrarlos a la consulta.

- Crear la consulta en la vista SQL.
  1. En **Microsoft Query**, haga clic en el botón **SQL** e introduzca la instrucción SQL, por ejemplo:

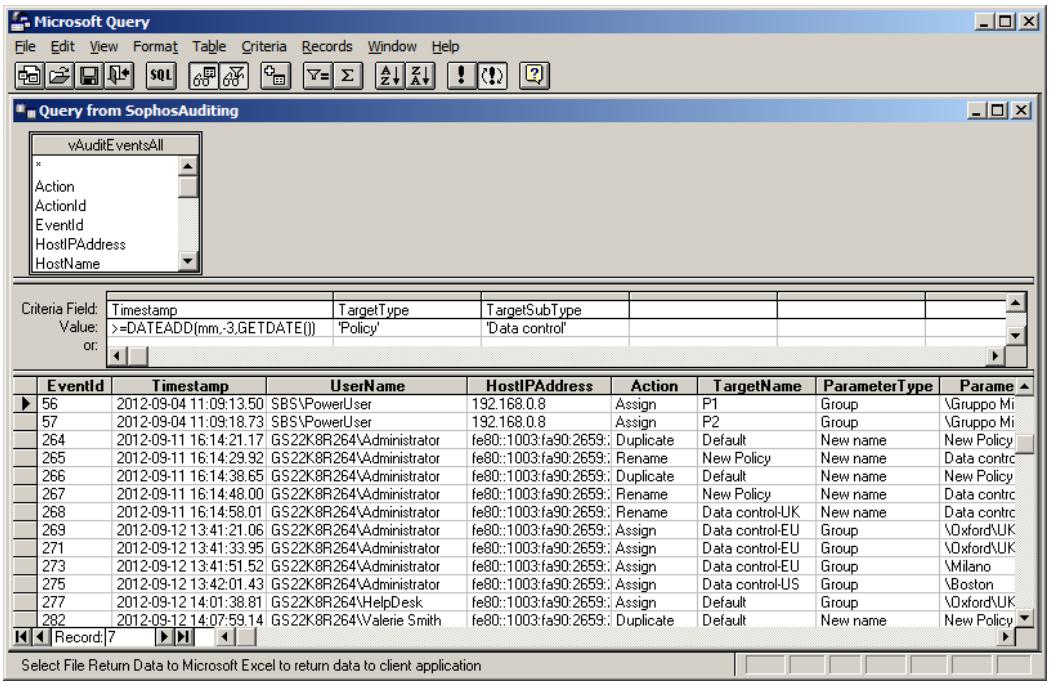
```
SELECT EventId, Timestamp, UserName, HostIPAddress, Action,
 TargetName, ParameterType, ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (TargetType='Policy')
AND (TargetSubType='Data control')

ORDER BY EventId ASC
```

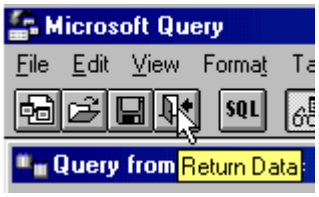
     Haga clic en **Aceptar**.



4. Para guardar la consulta, en el menú **Archivo**, seleccione **Guardar**.

7.3 Devolver datos a Excel

1. Para volver a Excel, en el cuadro de diálogo **Microsoft Query**, haga clic en **Devolver datos**.



   Si lo prefiere, en el menú **Archivo**, seleccione **Devolver datos a Microsoft Excel**.

   En Excel, aparece el cuadro de diálogo **Importar datos**, donde puede elegir el tipo de informe.

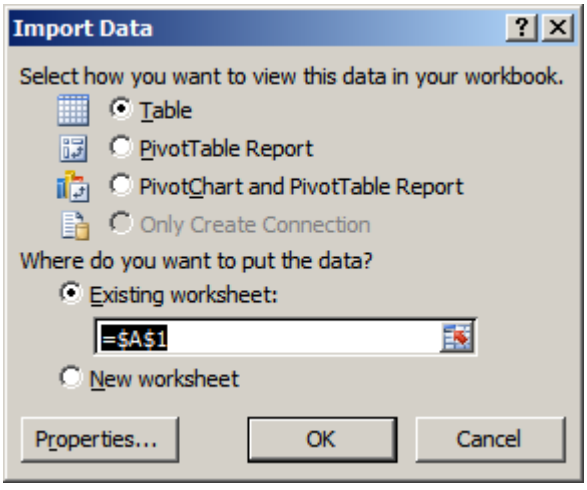
   En los siguientes ejemplos se muestra cómo:

   - Crear una tabla en la página 15
   - Crear un informe de tabla dinámica en la página 16

7.4 Crear una tabla

1. Si desea importar los datos de auditoría a una tabla de Excel, en el cuadro de diálogo **Importar datos**, seleccione la opción **Tabla**.

   Para insertar los datos en la hoja de cálculo abierta desde la celda A1, seleccione la opción **Hoja de cálculo existente**:

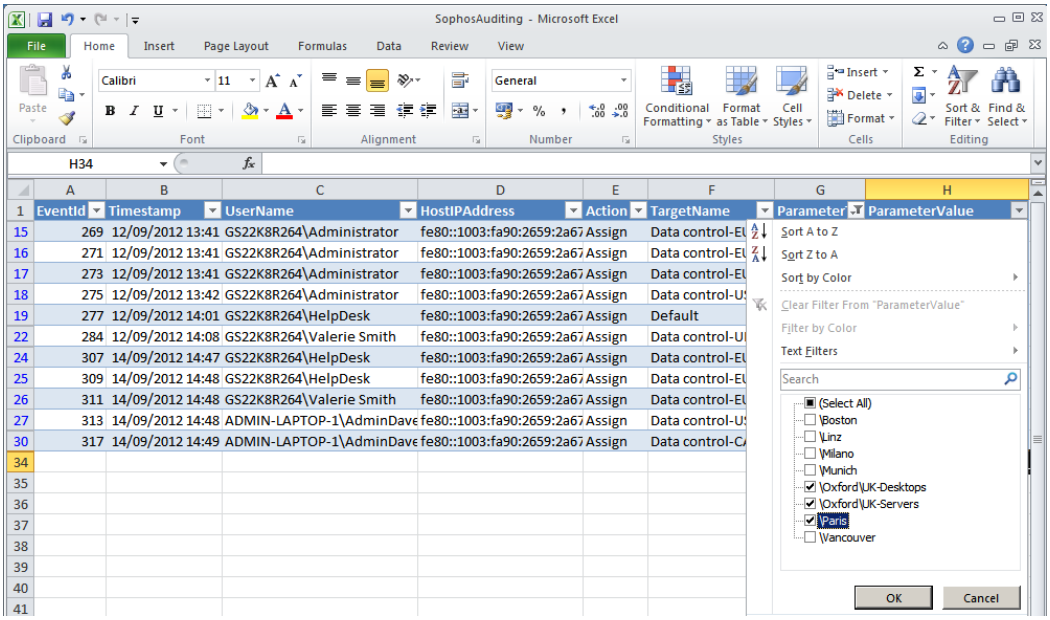


   Haga clic en **Aceptar**.

   Los datos de auditoría se importan a la tabla de Excel.

2. Guarde la hoja de cálculo.

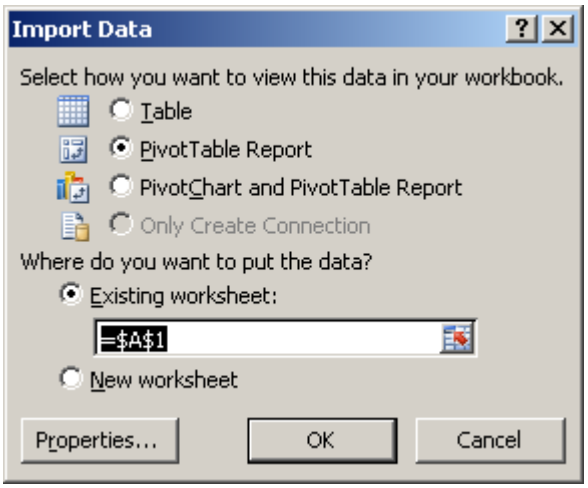
3. Utilice los filtros de búsqueda para analizar los datos.



7.5 Crear un informe de tabla dinámica

1. Si desea importar los datos de auditoría a una tabla de Excel, en el cuadro de diálogo **Importar datos**, seleccione la opción **Informe de tabla dinámica**.

   Para insertar los datos en la hoja de cálculo abierta desde la celda A1, seleccione la opción **Hoja de cálculo existente**:



   Haga clic en **Aceptar**.

   Se abre una tabla dinámica vacía en la hoja de cálculo.

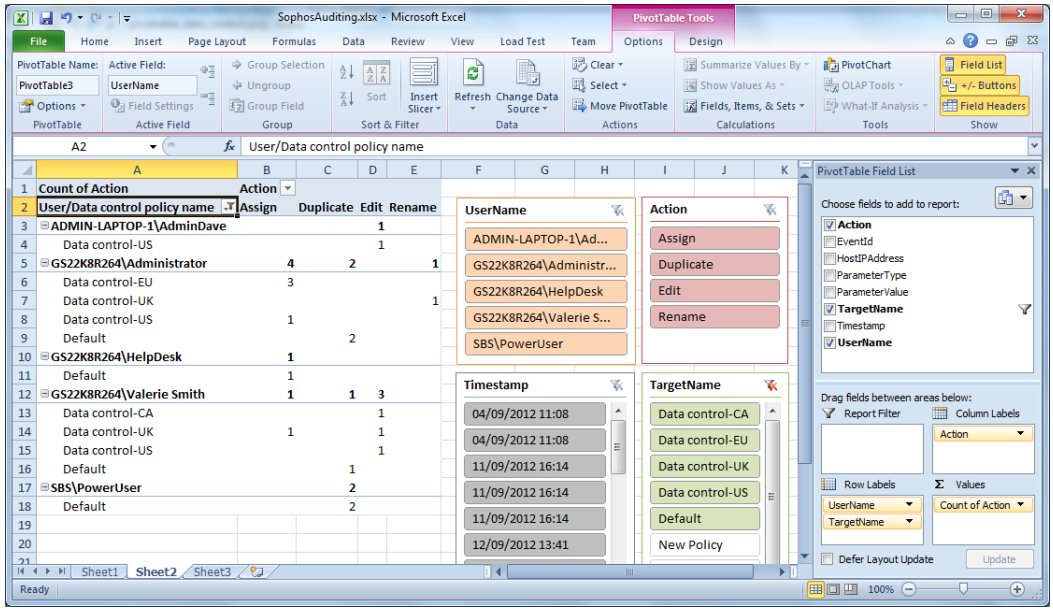
2. En la **Lista de campos de tabla dinámica** que aparece a la derecha, seleccione los campos que desee mostrar.

   Consejo: puede filtrar los datos antes de añadir los campos. En la **Lista de campos de tabla dinámica**, en el cuadro **Seleccionar campos para agregar al informe**, sitúe el puntero del ratón sobre el nombre del campo y haga clic en la flecha desplegable. En el menú **Filtro**, seleccione las opciones de filtrado.

3. Arrastre los campos a las diferentes áreas para obtener el efecto deseado de la **Lista de campos de tabla dinámica**. Por ejemplo, puede mostrar el nombre de los usuarios y las políticas modificadas como rótulos de fila y las acciones realizadas como rótulos de columna.
4. Para filtrar una tabla dinámica, en **Herramientas de tabla dinámica**, **Opciones**, haga clic en **Insertar segmentación**.
5. En el cuadro de diálogo **Insertar segmentación de datos**, seleccione la segmentación que desea utilizar y haga clic en **Aceptar**.

   Puede reajustar la segmentación moviéndola con el ratón. También puede personalizar la segmentación, por ejemplo, con diferentes colores. Para hacerlo, seleccione la segmentación. En **Herramientas de segmentación**, **Opciones**, seleccione el estilo deseado.

   Este es un ejemplo de tabla dinámica:



6. Guarde el libro.

8 Ejemplos de informes de auditoría

En esta sección se muestran ejemplos sobre cómo crear consultas en Microsoft Excel y cómo usar dichas consultas para crear informes de auditoría.

También se describe cómo crear un informe con información detallada de los cambios en las políticas en formato XML.

8.1 Crear una consulta de una fuente de datos

Para crear otro informe de auditoría a partir de la fuente de datos que ha creado en Configurar la conexión a la base de datos en la página 11:

1. En Excel, abra la ficha **Datos**, haga clic en **Desde otro origen** y seleccione **Desde Microsoft Query**.
2. En el cuadro de diálogo **Elegir origen de datos**, desactive la opción **Usar el Asistente para consultas para crear o modificar consultas**. Seleccione la fuente de datos que creó anteriormente (por ejemplo, SophosAuditing) y haga clic en **Aceptar**.
3. En **Microsoft Query**, haga clic en el botón **SQL** e introduzca la instrucción SQL para el informe.

A continuación se muestran algunos ejemplos.

8.2 Ejemplos de consultas

Ejemplo 1: Políticas modificadas por cierta persona en los últimos 60 días

```
SELECT EventId, Timestamp, TargetSubType, Action, TargetName,
ParameterType, ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(dd,-60,GETUTCDATE()))
AND (TargetType='Policy')
AND (UserName='GS22K8R264\Administrator')

ORDER BY Timestamp DESC
```

Nota: si desea incluir todos los campos en el informe, utilice "SELECT *".

Ejemplo 2: Políticas aplicadas a un grupo en los últimos 6 meses

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-6,GETUTCDATE()))
```

```
AND (TargetType='Policy')
AND (Action='Assign')
AND (ParameterType='Group')
AND (ParameterValue='\Oxford\UK-Servers')

ORDER BY EventId DESC
```

Nota: en el caso de subgrupos, puede indicar la ruta completa o utilizar la instrucción "termina con" (sólo si el nombre del grupo es único). Por ejemplo, para el grupo \Oxford\Servidores, puede utilizar:

- **`ParameterValue='\Oxford\Servidores'`**
- **`ParameterValue Like '%Servidores'`**

Ejemplo 3: Grupos modificados por cierta persona en los últimos 3 meses

El informe mostrará los grupos creados, borrados, movidos o cambiados de nombre, y los ordenadores asignados a grupos por el usuario indicado en los últimos 3 meses.

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (UserName='GS22K8R264\Administrator')
AND ((TargetType='Group') OR ((TargetType='Computer') AND
(Action='Assign')))
```

Ejemplo 4: Cambios en un grupo en los últimos 3 meses

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (ParameterValue='\Oxford\UK-Desktops')
```

8.3 Devolver datos a Excel

Tras crear la consulta para el informe de auditoría, devuelva los datos a Excel (**Archivo** > **Devolver datos a Microsoft Excel**) y cree el informe como se describe en Crear una tabla en la página 15 o Crear un informe de tabla dinámica en la página 16.

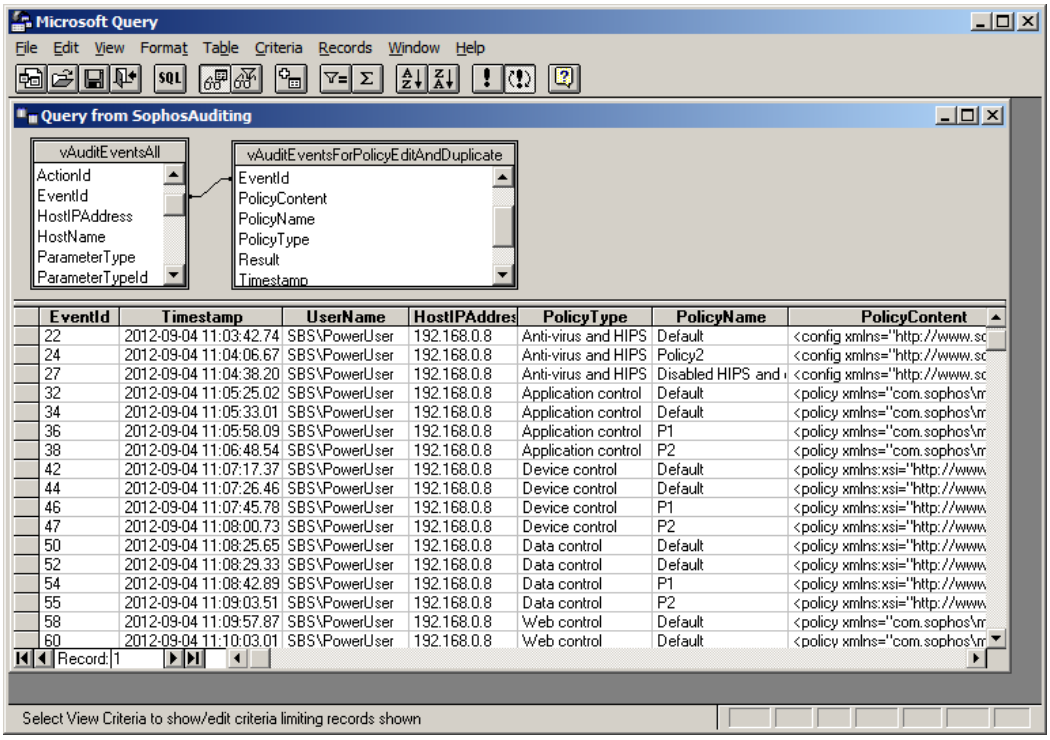
8.4 Crear un informe con los cambios de las políticas en formato XML

Cuando se modifica una política, la configuración se guarda en formato XML y se puede consultar mediante la vista de la base de datos **Reports.vAuditEventsForPolicyEditAndDuplicate**.

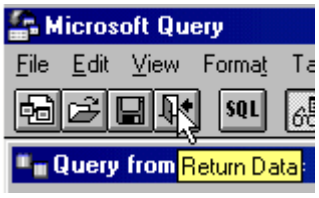
Es posible crear un informe con estos datos vinculando dos tablas: **Reports.vAuditEventsAll** y **Reports.vAuditEventsForPolicyEditAndDuplicate**.

1. Cree una nueva consulta a partir de una fuente de datos existente, tal como se describe en Crear una consulta de una fuente de datos en la página 18.
2. En **Microsoft Query**, haga clic en **Tabla** y seleccione **Agregar tablas**. En el cuadro de diálogo **Agregar tablas**, seleccione **vAuditEventsForPolicyEditAndDuplicate** y haga clic en **Agregar**. Haga clic en **Cerrar**.
3. Vincule las tablas entre sí mediante los campos comunes. Seleccione el campo común **EventID** en una tabla y arrástrelo al campo **EventID** en la otra tabla.
4. Añada los campos a la consulta. Puede hacer doble clic o arrastrarlos a la consulta.

   Consejo: puede utilizar el cuadro de diálogo **Uniones** en Microsoft Query (**Tabla** > **Uniones**) para crear una consulta que una las dos tablas.



5. Para guardar la consulta, en el menú **Archivo**, seleccione **Guardar**.
6. Para volver a Excel, haga clic en el botón **Devolver datos**.



   Si lo prefiere, en el menú **Archivo**, seleccione **Devolver datos a Microsoft Excel**.

   En Excel, aparece el cuadro de diálogo **Importar datos**. Cree una tabla (Crear una tabla en la página 15). La columna **PolicyContent** incluirá los cambios en la política en formato XML.

   Consejo: si utiliza Microsoft SQL Server Management Studio, puede consultar directamente la vista **Reports.vAuditEventsForPolicyEditAndDuplicate**. Al hacer clic en el resultado de la columna **PolicyContent**, el contenido de la política se mostrará en un editor XML.

9 Acciones en la auditoría

Las acciones que entran en la auditoría corresponden a las siguientes categorías:

- Acciones sobre ordenadores
- Gestión de grupos de ordenadores
- Gestión de políticas
- Gestión de roles
- Gestión de Sophos Update Manager
- Eventos del sistema

9.1 Acciones sobre ordenadores

Se registran las siguientes acciones sobre ordenadores:

- Quitar y resolver alertas y errores
- Proteger un ordenador
- Actualizar un ordenador
- Eliminar un ordenador
- Realizar escaneados remoto

9.2 Gestión de grupos de ordenadores

Las acciones registradas de la administración de grupos son:

- Crear un grupo
- Eliminar un grupo
- Mover un grupo
- Cambiar el nombre de un grupo
- Asignar un ordenador a un grupo

9.3 Gestión de políticas

Las acciones registradas de la administración de políticas son:

- Crear una política en la página 22
- Cambiar el nombre de una política
- Duplicar una política en la página 22
- Editar políticas
- Asignar una política a un ordenador
- Restaurar una política a las opciones predeterminadas

- Eliminar una política en la página 22

9.3.1 Crear políticas

Al crear una política nueva, se duplica la política predeterminada con el nombre "Nueva política". A continuación puede cambiar el nombre de la política nueva. Por ejemplo, al crear una política Antivirus y HIPS nueva y cambiarle el nombre a "Servidores", se registrarán las siguientes entradas:

Tabla 1: Crear una política nueva y establecer el nombre

Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
Duplicate	Policy	Anti-virus and HIPS	Default	New name	New Policy	Success
Rename	Policy	Anti-virus and HIPS	New Policy	New name	Servers	Success

9.3.2 Duplicar una política

Al duplicar una política, se registra la acción de duplicar una política, por ejemplo:

Tabla 2: Duplicar una política

Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
Duplicate	Policy	Web Control	TestPolicy1	New name	Copy of TestPolicy1	Success

9.3.3 Borrar políticas

Al borrar una política, todos los grupos que utilizaban dicha política pasarán a utilizar la política predeterminada. En este caso, no se registra la aplicación de la política predeterminada.

9.4 Gestión de roles

Las acciones registradas de la administración de roles son:

- Crear roles
- Borrar roles
- Cambiar el nombre de roles
- Duplicar un rol
- Añadir usuarios a roles

- Eliminar usuarios de roles
- Añadir permisos a roles
- Eliminar permisos de roles

9.5 Gestión de Sophos Update Manager

Las acciones registradas de la administración de Sophos Update Manager son:

- Actualizar el gestor de actualización
- Hacer que el gestor cumpla con la configuración
- Quitar alertas
- Eliminar un gestor de actualización
- Configurar el gestor de actualización

9.5.1 Cómo se registran los cambios en la configuración del gestor de actualización

En Enterprise Console, el cuadro de diálogo **Configuración del gestor de actualización** contiene diferentes fichas con las opciones de configuración que determinan las políticas del gestor de actualización. Al modificar las opciones de configuración del gestor de actualización, se registran las acciones en las siguientes políticas:

- **Update Manager - subscription**, que especifica las suscripciones de software.
- **Update Manager - upstream**, que determina la fuente de actualización.
- **Update Manager - downstream**, que controla la ubicación de descarga.
- **Update Manager - schedule**, que especifica la frecuencia de las actualizaciones del software y datos de detección.
- **Update Manager - general**, que determina las opciones de registro.
- **Software subscription**, que especifica la configuración de la suscripción, por ejemplo, "Recommended".

Es posible que cambios en una política afecten a otras políticas (como cambios del identificador). En este caso, se mostrarán varias entradas provocadas por un cambio. Por ejemplo, si crea una actualización programada en la ficha **Actualización automática** del cuadro de diálogo **Configuración del gestor de actualización**, se crearán las siguientes entradas de auditoría:

Tabla 3: Crear una actualización programada en el gestor de actualización

EventId	Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
22	Edit	Policy	Update Manager - schedule	New name	None		Success

EventId	Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
21	Edit	Policy	Update Manager - upstream	New Policy	None		Success
20	Edit	Policy	Update Manager - subscription		None		Success

En este caso, sólo la primera acción, registrada en la política **Update Manager - schedule**, es consecuencia directa del cambio. El resto de eventos se producen como consecuencia de cambios internos en el parámetro de identificación. Para revisar cuáles son los cambios, puede utilizar la vista **Reports.vAuditEventsForPolicyEditAndDuplicate** de la base de datos de SophosSecurity, tal como se describe en Crear un informe con los cambios de las políticas en formato XML en la página 19.

9.6 Eventos del sistema

Se registran los siguientes eventos del sistema:

- Activar la auditoría
- Desactivar la auditoría

10 Campos de datos de Sophos Auditing

Sophos Auditing dispone de las siguientes vistas de la base de datos o fuentes de datos:

- Reports.vAuditEventsAll
- Reports.vAuditEventsForPolicyEditAndDuplicate

A continuación se listan los campos de datos disponibles en cada vista. Los datos del tipo datetime se ofrecen en hora universal UTC con el formato "aaaa-mm-dd hh:mi:ss" (24 horas). En negrita se indican los campos comunes.

Reports.vAuditEventsAll

La vista **Reports.vAuditEventsAll** contiene todos los eventos de auditoría y la mayor parte de la información.

Campo de datos	Tipo	Descripción
EventId	integer	Identificador numérico del evento.
Timestamp	datetime	Fecha y hora en que se realizó la acción.
Action	nvarchar(128)	Acción que se llevó a cabo, por ejemplo, Create, Edit, Rename, Assign, Delete.
TargetType	nvarchar(128)	Tipo de objeto u opción modificados, por ejemplo, Group, Computer, Policy, Role.
TargetSubType	nvarchar(128)	El subtipo del objeto u opción modificados (si procede). Por ejemplo, el nombre de la política, como Antivirus y HIPS o Control de datos.
TargetName	nvarchar(4000)	Nombre del objeto u opción modificados, por ejemplo, el nombre asignado por el usuario a una política o grupo.
ParameterType	nvarchar(128)	El tipo de nueva configuración u objeto asignado al destino. Por ejemplo, para Action="Rename" y TargetType="Policy", ParameterType="New name". Para Action="Assign" y TargetType="Computer", ParameterType="Group".
ParameterValue	nvarchar(4000)	Valor del objeto u opción nuevos, por ejemplo, el nuevo nombre que el usuario asigna a una política o el grupo nuevo al que se asigna un ordenador.
Result	nvarchar(128)	Resultado de la acción: "Success" o "Failure".

Campo de datos	Tipo	Descripción
UserName	nvarchar(256)	Nombre del usuario que realizó la acción.
HostName	nvarchar(256)	Nombre del equipo en el que se llevó a cabo la acción.
HostIPAddress	nvarchar(48)	Dirección IP del equipo en el que se llevó a cabo la acción. Si utiliza IPv6, se registrará este tipo de dirección IP. De lo contrario, se registrará la dirección IPv4.
ActionId	integer	Identificador numérico de la acción.
TargetTypeId	integer	Identificador numérico del tipo de destino.
TargetSubTypeId	integer	Identificador numérico del subtipo de destino.
ParameterTypeId	integer	Identificador numérico del tipo de parámetro.
SubEstateId	integer	Identificador numérico del subentorno del usuario.
ResultId	integer	Identificador numérico del resultado: 1 (success), 0 (failure).
UserSid	nvarchar(128)	Identificador de seguridad del usuario.

Reports.vAuditEventsForPolicyEditAndDuplicate

La vista **Reports.vAuditEventsForPolicyEditAndDuplicate** contiene información sobre los cambios de las políticas.

Campo de datos	Tipo	Descripción
EventId	integer	Identificador numérico del evento.
Timestamp	datetime	Fecha y hora en que se realizó la acción.
Action	nvarchar(128)	Acción registrada en el evento.
Result	nvarchar(128)	Resultado de la acción: "Success" o "Failure".

Campo de datos	Tipo	Descripción
PolicyType	nvarchar(128)	Tipo de política modificada, por ejemplo, Antivirus y HIPS o Control web.
PolicyName	nvarchar(4000)	Nombre asignado por el usuario a la política.
PolicyContent	XML	Fragmento de los cambios de la política en formato XML.
UserName	nvarchar(256)	Nombre del usuario que realizó la acción.

11 Solución de problemas

Si se produce algún error en Sophos Auditing, se incluirá en el registro de eventos de aplicación de Windows con el nombre "Sophos Auditing". Esto puede ocurrir por algún problema de conexión con la base de datos.

12 Apéndice: Identificadores numéricos de los valores de campos de datos

La siguiente tabla muestra los identificadores numéricos de algunos de los valores de campos de datos de Sophos Auditing.

Se recomienda utilizar los identificadores numéricos en vez de la cadena del valor para realizar enlaces lógicos con los datos obtenidos. De esta forma evitará problemas de compatibilidad con próximas ediciones de Enterprise Console.

Campo de datos	Valor del campo de datos	Identificador
Action	Unknown	0
	Create	1
	Delete	2
	Duplicate	3
	Move	4
	Rename	5
	Add to	6
	Remove from	7
	Edit	8
	Log on	9
	Update	10
	Acknowledge	11
	Reset	12
	Assign	13
	Protect	14
	Scan	15
	Clean up	16
	Comply	17

Campo de datos	Valor del campo de datos	Identificador
TargetType	Unknown	0
	Group	1
	Role	2
	Policy	3
	Computer	4
	Sub-estate	5
	AD synchronization point	6
	Report	7
	Update manager	8
	Configuration	9
TargetSubType for TargetType=Policy	Legacy updating	1
	Anti-virus and HIPS	2
	Firewall	4
	Application control	7
	NAC	8
	Update Manager - upstream	9
	Update Manager - downstream	10
	Update Manager - general	11
	Update Manager - subscription	12
	Update Manager - schedule	13
	Data control	15
	Device control	16
	Software subscription	17
	Updating	18
	Tamper protection	19

Campo de datos	Valor del campo de datos	Identificador
	Web control	22
	Prevención de vulnerabilidades	El 30
TargetSubType for TargetType=Configuration	Unknown	0
	Dashboard	1
	Email alerts	2
	Purge	3
	Auditing	4
ParameterType	None	0
	New name	1
	New location	2
	Group	3
	User/Group	4
	Right	5
	Computer	6
	Alert	7
	Error	8
	Software update alert	9
	Configuration value	10
Result	Pending	0
	Success	1
	Failure	2

13 Soporte técnico

Para obtener asistencia técnica sobre cualquier producto de Sophos, puede:

- Visitar la comunidad de Sophos en community.sophos.com/ para consultar casos similares.
- Visitar la base de conocimiento de Sophos en www.sophos.com/es-es/support.aspx.
- Descargar la documentación correspondiente desde www.sophos.com/es-es/support/documentation.aspx.
- Abrir un ticket de incidencia con nuestro equipo de soporte en https://secure2.sophos.com/support/contact-support/support-query.aspx.

14 Aviso legal