centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1207

Procedimiento de empleo seguro
Sophos Intercept X Advanced

Diciembre 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.12.18 15:19:30 +01'00'

NIPO: 083-20-190-8

Fecha de Edición: Diciembre de 2020

ÍNDICE

1. INTRODUCCIÓN

1. ***Sophos Intercept X Advanced*** es una herramienta de antivirus y EDR (*Endpoint Detection and Response*) que presenta las siguientes funcionalidades:
    a) Protección antimalware basada en:
        a. Firmas.
        b. *Deep Learning* (inteligencia artificial).
        c. Consultas a Sophos Labs en tiempo real.
        d. *AntiExploit*.
        e. Control de comportamiento.
        f. Detección de técnicas post-explotación.
    b) EDR.
    c) Control de navegación web.
    d) Control de dispositivos.
    e) Control de aplicaciones.
    f) Gestión del *firewall* de Windows.
    g) Prevención de fuga de datos.
    h) Control de actualizaciones.
    i) Bloqueo de servidores.
    j) Detección de cambio de ficheros.
2. Las funcionalidades son gestionado desde una consola en nube, **Sophos Central**, la cual además sirve para la gestión del resto del portfolio de Sophos, como seguridad de red (*Sophos XG Firewall*), seguridad de correo (*Sophos Central Email*), cifrado de equipos (*Sophos Centran Device Encryption*), gestión y protección de móviles (*Sophos Central Mobile*), educación de usuarios (*Sophos PhishThreat*), *Cloud Secure Posture Management (Sophos Cloud Optix*) y redes inalámbricas (*Sophos Cloud Wireless*).
3. La solución puede ser empleada en equipos *endpoint* y servidor Windows, Windows Server, MacOS y Linux.

2. OBJETO Y ALCANCE

4. El propósito del presente documento es detallar las configuraciones de seguridad del producto **Sophos Intercept X Advanced versión 10.8.6**, para que su protección y funcionamiento se realice de acuerdo a unas garantías mínimas de seguridad.

5. *Sophos Intercept X Advanced* es un producto software cuya instalación se realiza en los dispositivos que desea proteger, mediante el uso de agentes.

3. ORGANIZACIÓN DEL DOCUMENTO

6. Este documento está organizado en diferentes capítulos, de acuerdo a diferentes fases del ciclo de vida del producto:

   a) **Apartado 4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

   b) **Apartado 5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   c) **Apartado 6**. En este apartado se recogen las tareas recomendadas para la fase de operación y mantenimiento del producto.

   d) **Apartado 7.** En este apartado se incluye un *checklist* para verificar las tareas de configuración segura mencionadas a lo largo del documento.

   e) **Apartado 8.** Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

   f) **Apartado 9.** Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE DE INSTALACIÓN

7. La instalación del producto se realiza a través de la consola de gestión de Sophos Central. El acceso a la misma se realiza a través del portal *https://central.sophos.com*, accesible mediante navegador web utilizando HTTPS y cuyo certificado es:

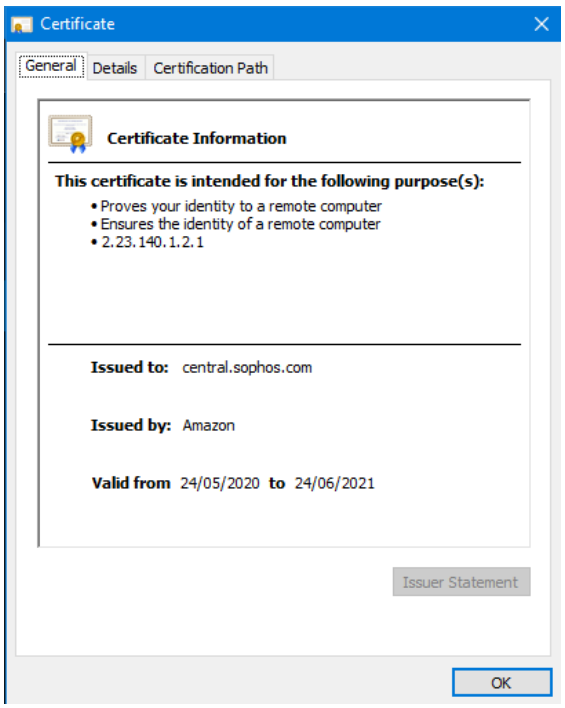

Ilustración 4-1. Certificado del portal Sophos Central

8. El acceso a la consola se realiza con un usuario suministrado por el fabricante a través de correo electrónico. La contraseña es generada por el propio usuario. El usuario deberá tener en cuenta las restricciones y recomendaciones de seguridad detalladas en el apartado 5.2 Autenticación.

9. Este primer usuario generado tendrá el rol de "*superadministrador*" y será el que genere sucesivos usuarios. De igual forma, el sistema envía un correo de confirmación, para que sea el propio usuario el que genere su contraseña.

10. La ruta de certificación es:

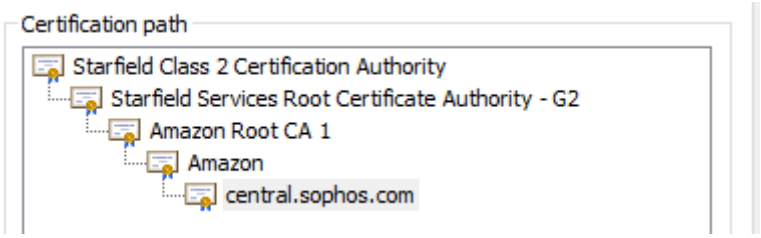

Ilustración 4-2. Ruta del certificado de la consola de gestión

11. La descarga del instalador de los agentes utilizados para proteger los dispositivos finales se realiza desde el menú *Protect Devices* (Protección de Dispositivos):

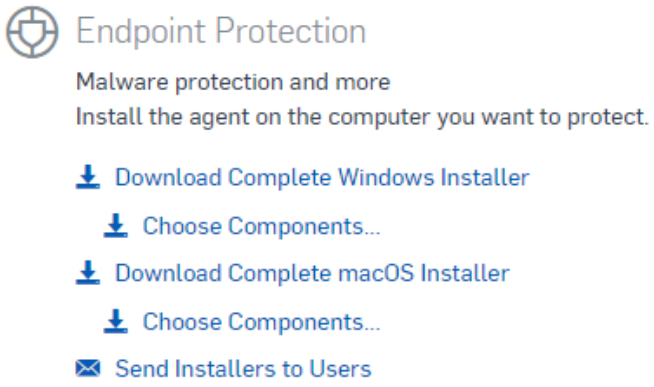

Ilustración 4-3. Descarga del instalador de los agentes

12. Las opciones *Download Complete Windows Installer* y *Download Complete macOS Installer* proporcionan un instalador para dispositivos Windows y macOS respectivamente, con todos los productos para *endpoint* incluidos en la licencia obtenida por la organización.
13. La opción de *Choose Components*, bajo cada una de las opciones recién mencionadas, permite seleccionar un instalador solo con los productos deseados, para cada tipo de dispositivo.
14. Se puede verificar la autenticidad del fichero *.EXE del agente descargado comprobando que este se encuentra firmado utilizando el siguiente certificado:

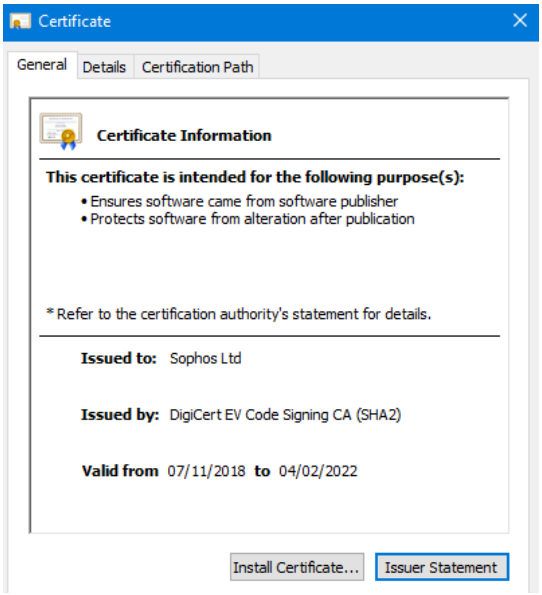

Ilustración 4-4. Certificado del agente

4.1 ENTORNO DE INSTALACIÓN SEGURO

15. Dado que *Sophos Central Intercept X* es un producto cuya consola de gestión está basada en nube, sólo es necesario desplegar los agentes en los equipos a proteger.

16. En caso de que no exista conexión directa a internet o nos encontremos ante redes aisladas o muy restringidas, es posible seleccionar aquellos dispositivos que queramos configurar como:

    - ***Update Cache***: usará el puerto TCP 8191 para actuar como servidor de actualizaciones de firmas y motores para los dispositivos en la red de la organización (ver apartado 5.5 Actualizaciones).
    - ***Message Relay***: usará el puerto TCP 8190 para hacer de *proxy* de mensajería entre los equipos y la nube de Sophos Central.

17. El despliegue de los elementos anteriores permite centralizar las actualizaciones y las comunicaciones en aquellas ubicaciones (típicamente *datacenters*) que se desee, o incluso definir estas parejas por cada delegación, centralizando así tráficos y ahorrando anchos de banda.

18. Para configurar un Update Cache o un Message Relay, se accede a central.sophos.com:

    - Ir a Settings > Manage Update Caches and Message Relays.
    - En el filtro sobre la tabla, seleccionar '*Cache Capable Servers*' para ver qué servidores tienen la capacidad de actuar como alguno de estos componentes. Dichos servidores serán los que previamente tengan instalado el agente de *endpoint* de *Sophos*. Además necesitan cumplir los siguientes prerrequisitos técnicos:

      https://support.sophos.com/support/s/article/KB-000035498?language=en_US
    - Seleccionar el servidor o servidores que se desea configurar como *Cache* o *Relay*.
    - Hacer clic en 'Set Up Cache/Relay'.

19. Una vez seleccionados los servidores, el producto configura de forma automática los dispositivos en la red de la organización para utilizar el *Update Cache* o *Message Relay* creado. También pueden asignarse los dispositivos a un *Cache/Relay* de forma manual:

    - Ir a Settings > Manage Update Caches and Message Relays.
    - Para el servidor elegido, seleccionar el enlace que muestra el número de dispositivos utilizando dicho *Cache/Relay*.
    - Hacer clic en 'Manual Assignment'.
    - Seleccionar los dispositivos deseados.
    - Hacer clic en '*Save'.*

20. El detalle de la configuración de *Update Caches* y *Message Relays* se puede consultar en el apartado correspondiente de la guía *Sophos Central Admin Help* [REF1].

4.2 REGISTRO Y LICENCIAS

21. La adquisición de licencias se hace a través de la red de *partners* certificados de Sophos. Una vez adquirida la licencia, se recibirá un email que incluirá un PDF con los códigos de activación, los cuales, se introducirán en la zona de gestión de licencia de Sophos Central. Para ello, se debe seleccionar el nombre de la cuenta, en la parte superior izquierda y haciendo clic sobre '*Licensing*':

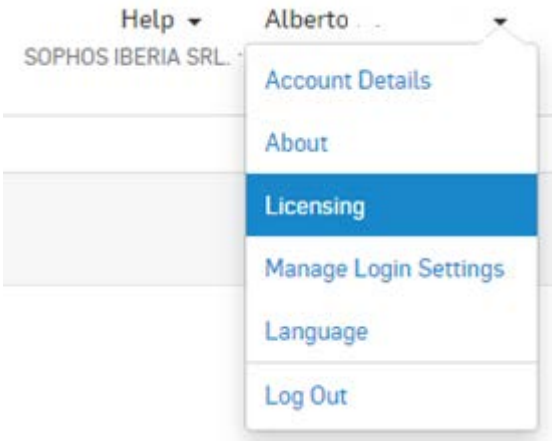

Ilustración 4-5. Zona de gestión de licencias de Sophos Central

22. Aparecerá entonces la opción de introducir la licencia para activar las funcionalidades:

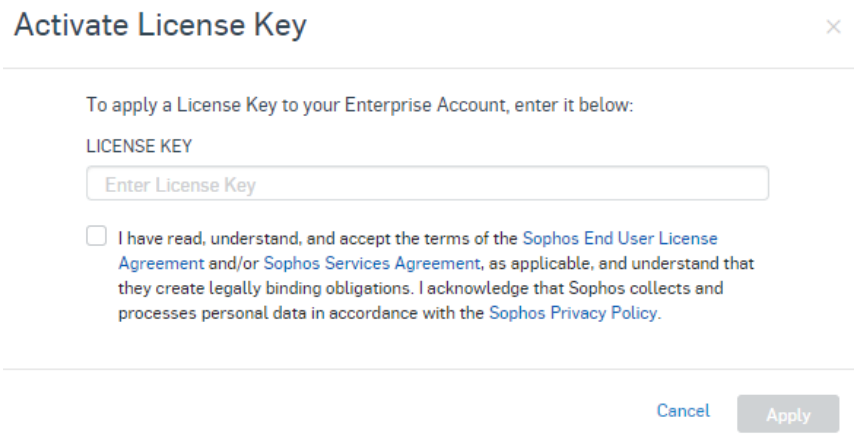

Ilustración 4-6. Página de introducción de licencias.

23. Las licencias de Sophos permiten el uso del producto hasta su fecha de expiración, permitiendo actualizar a las nuevas versiones según estén disponibles, sin atar a la organización a una versión concreta.

4.3 CONSIDERACIONES PREVIAS

24. Todas las comunicaciones de los *endpoints* contra central.sophos.com se establecen a través del puerto 443. Dicha comunicación no puede ser interceptada mediante HTTPS *inspection* o similar, ya que si el certificado que llega al endpoint no es el original de Sophos, la comunicación no se establece. Esto es así para evitar

ataques *Man in the middle*, por lo que, si existe ese tipo de análisis web, se deben de realizar las exclusiones correspondientes a las URL que se indican en los siguientes puntos.

25. Como se ha comentado en el punto 4.2 Entorno de instalación seguro es posible tener equipos que no dispongan de conexión a Internet gracias al uso de los *Update Cache* y *Message Relay*. Se necesitará que al menos éstos sí dispongan de acceso a los servicios de Sophos por los puertos TCP 80 y TCP 443, desde la red de la organización a los recursos listados a continuación:

    *.sophos.com

    *.sophosupd.com

    *.sophosupd.net

    *.sophosxl.net

    ocsp2.globalsign.com

    crl.globalsign.com

26. Si no fuese posible realizar excepciones de los *firewalls/proxies* con "*", la lista completa de dominios puede encontrarse en https://docs.sophos.com/central/Customer/help/en-us/central/Customer/concepts/DomainsPorts.html

27. Respecto a las características que deben cumplir los equipos:

    - Los equipos Windows *Endpoint* deberán disponer de las siguientes características:

Platforms support	Endpoint Protection	Intercept X	Intercept X Advanced	Intercept X Advanced with EDR	Intercept X Advanced with EDR and MTR
Windows 7,8,8.1 and 10	Disk space: 2 GB free RAM: 2 GB Cores: 2	Disk space: 2 GB free RAM: 2 GB Cores: 2	Disk space: 4 GB free RAM: 4 GB Cores: 2	Disk space: 8 GB free RAM: 4 GB Cores: 2	Disk space: 8 GB free RAM: 4 GB Cores: 2

Ilustración 4-7. Requisitos generales dispositivos Windows Endopoint

CPU utilization	Description
< 0.1%	When deployed and protecting a lightly used machine and recording activity for future Threat Case generation.
< 2%	When actively monitoring a suspect activity like installing new software, evaluating a process for ransom conviction/exoneration and recording activity for Threat Case.
Up to 1%	Utilization immediately after a detection as Threat Case data collection runs and cleanup is actively removing the components of the attack.

Ilustración 4-8. Requisitos CPU dispositivos Windows Endopoint

Memory utilization	Description
150-200 MB	Most of this is the Sophos Data Recorder (100MB) that is collecting activity events for use when a Threat Case report is required

Ilustración 4-9. Requisitos memoria dispositivos Windows Endopoint

- Los dispositivos Windows Server deberán disponer de:

Platforms supported	Server Protection	Intercept X Advanced for Server	Intercept X Advanced for Server with EDR
Windows Server 2008 R2, SBS 2011, 2012. 2012 R2, 2016 and 2019	Disk space: 5 GB free RAM: 4 GB Cores: 2	Disk space: 8 GB free RAM: 8 GB Cores: 2	Disk space: 10 GB free RAM: 8 GB Cores: 2
Windows Server 2008 (32-bit or 64-bit)	Disk space: 2 GB minimum RAM: 2 GB minimum Cores: 2	Unsupported	Unsupported

Ilustración 4-10. Requisitos generales dispositivos Windows Server.

- Los dispositivos Linux deberán disponer de:
  - Distribuciones soportadas :
    - *Amazon Linux, Amazon Linux 2*
    - *CentOS 6/7/8*
    - *Debian 9, 10*
    - *Oracle Linux 6/7/8*
    - *Red Hat Enterprise Linux 6/7/8*
    - *SUSE 12/15*
    - *Ubuntu 16/18 LTS*
  - Tipo de sistema: *x86_64*
  - Versión de la biblioteca: biblioteca C de GNU (Glibc) 2.11+
  - la versión del núcleo: *Kernel 2.6.32+*
  - Espacio Libre: 1 GB
  - Memoria Libre: 1 GB
  - Tamaño de las pilas: no se admiten tamaños no predeterminados.
  - Versión del idioma: inglés y japonés (EUC y UTF-8). *Shift JIS* y *JIS* no son compatibles.

- En el caso de los contenedores *Docker*, no se puede garantizar una cobertura del 100% en el acceso de los archivos dentro de los contenedores por lo que no se admite su escaneado.

- Los dispositivos MacOS deberán disponer de:

Platforms support	Endpoint Protection	Intercept X Advanced (MTR Included)
MacOS 10.13, 10.14 and 10.15 Intel-based Macs (64-bit)	Disk space: 2 GB free RAM: 2 GB	Disk space: 2 GB free RAM: 2 GB

Ilustración 4-11. Requisitos generales dispositivos MacOS.

4.4 INSTALACIÓN

28. Cada instalador esta personalizado para cada cliente, por lo tanto, una vez descargado desde la consola de central y seguido el punto 4.1 Entrega segura del producto, se procederá a la ejecución del agente en el dispositivo *endpoint* en cuestión.

29. En caso de necesitar una instalación personalizada, es posible añadir ciertos modificadores como, por ejemplo:

- Que la instalación sea silenciosa y no interactiva (este va por defecto)

Quiet	
Example usage	`--quiet`
Description	Runs the installer without displaying the user interface.
Trailing argument	Not available

- Si vamos a usar un *relay* y no queremos que el *endpoint* vaya a Sophos Central.

Message Relays	
Example usage	`--messagerelays=<comma-separated message relay list of IPs including the port>`
Description	Specifies a list of message relays to use.
Trailing argument	The IP address of the message relay must be specified along with the port 8190. Example: --messagerelays=IPADDRESS:8190

Ilustración 4-12. Ejemplo de modificadores del instalador

30. La lista completa se puede consultar en:

    https://support.sophos.com/support/s/article/KB-000036839?language=en_US

31. Si se desee realizar un despliegue en multitud de dispositivos de forma simultánea, Sophos diversos métodos para ello según las plataformas disponibles indicadas en el siguiente enlace:

    https://support.sophos.com/support/s/article/KB-000034831?language=es_ES

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

32. Una vez que se ha desplegado el *software*, el equipo queda configurado con las opciones por defecto, pero con ciertas protecciones deshabilitadas (como, por ejemplo, el control de aplicaciones y el control de dispositivos). **Se deben crear políticas para la activación y gestión de las protecciones.**

33. Estas políticas se configuran en la plataforma Sophos Central, desde la sección '*Policies*', haciendo clic en '*policy type*' y seleccionando aquella que quiera configurarse.

34. Se debe realizar la siguiente configuración para la política de protección contra amenazas (*Threat Protection Policy*):

- Desmarcar el botón de "*use recommended settings*":

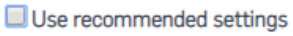

Ilustración 5-1. Deshabilitar la opción de configuración recomendada

- Una vez desmarcado, activar, si no estuviese, el *Deep Learning*:

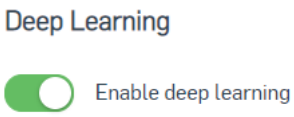

Ilustración 5-2. Activación de *Deep Learning*

- Verificar que *Real Time Scanning* se encuentra activo y que realiza el análisis de ficheros remotos:

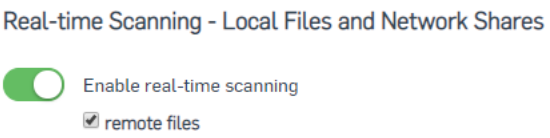

Ilustración 5-3. Activación de *Real Time Scanning*

- Verificar también que los análisis en tiempo real estén activados para las descargas de Internet:

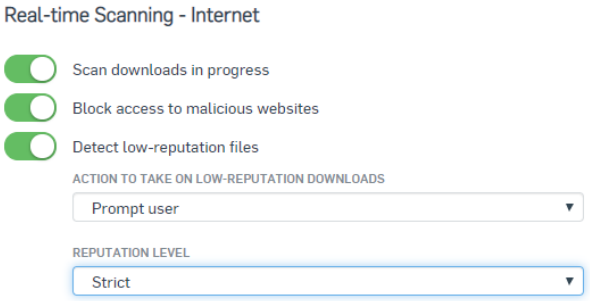

Ilustración 5-4. Activación *Real Time Scanning* en las descargas de internet

- Adicionalmente, verificar que la remediación esté activa, para así no sólo detectar, sino limpiar las amenazas detectadas:

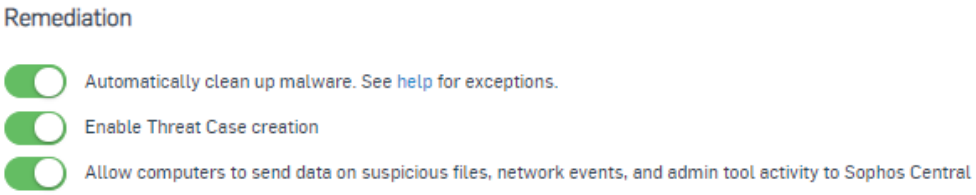

Ilustración 5-5. Activación de la remediación de amenazas detectadas.

- Activar también todas las protecciones en tiempo de ejecución:

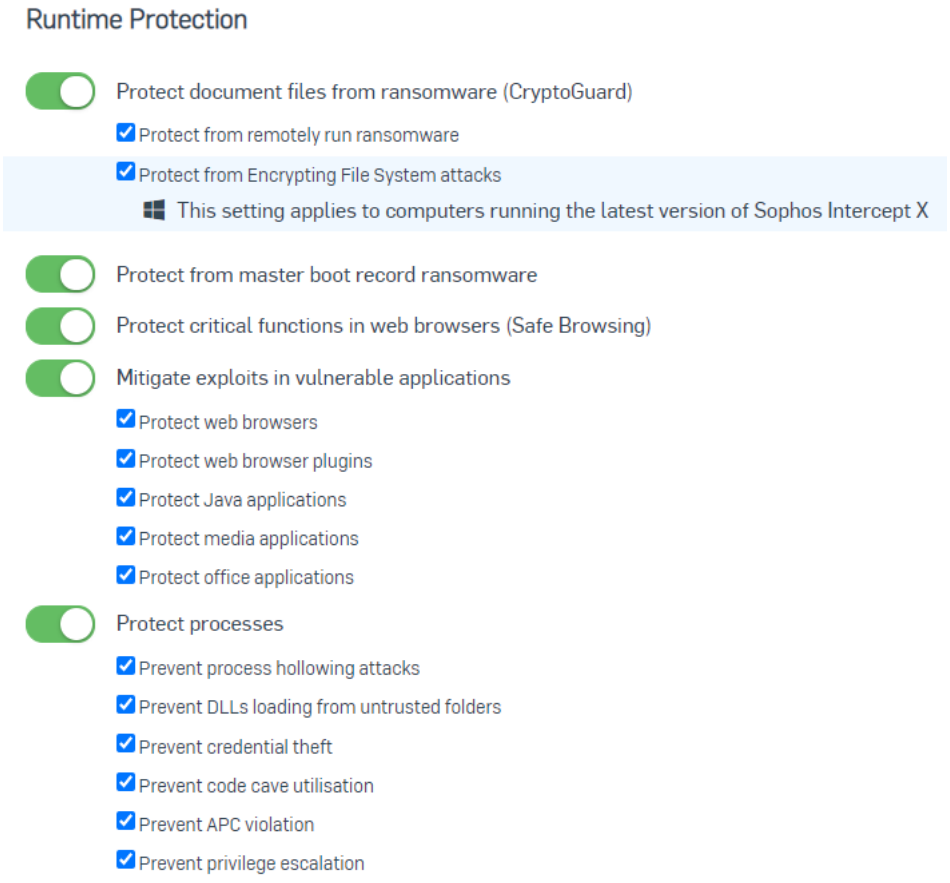

Ilustración 5-6. Activación de las protecciones en tiempo real (1)

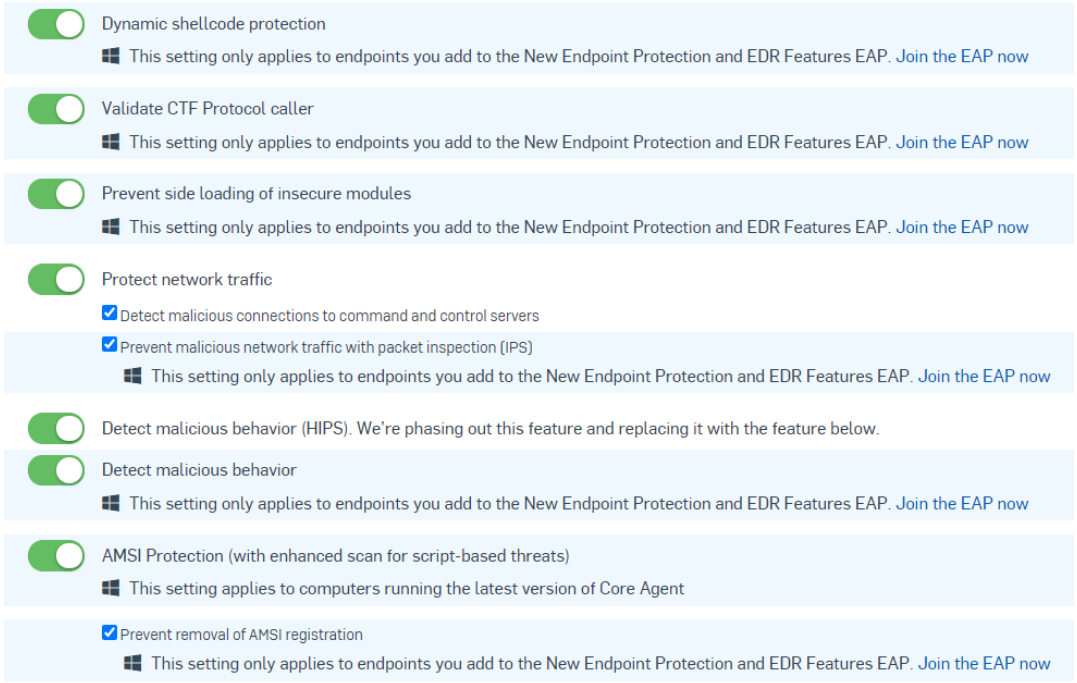

Ilustración 5-7. Activación de las protecciones en tiempo real (2)

- Activar también el aislamiento de equipos, de tal modo que, en caso de encontrar una amenaza, el equipo bloqueará todas las conexiones salientes y entrantes:

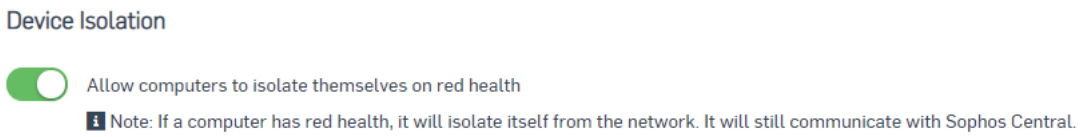

Ilustración 5-8. Activación del aislamiento de equipos

- Finalmente, activar al menos un escaneo de los dispositivos programado a la semana:

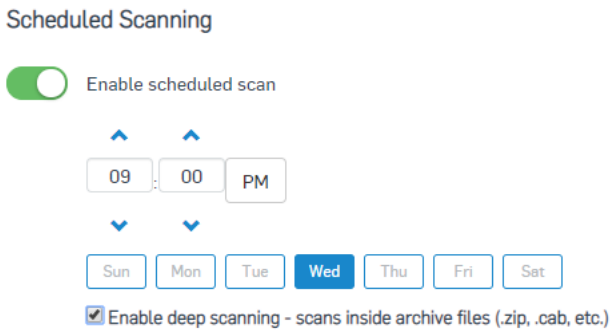

Ilustración 5-9. Programación del escaneo periódico

35. Se debe realizar la siguiente configuración para la política de gestión de dispositivos (*Peripheral Control Policy*):

- Activar el modo monitor '*Monitor but do not block*', para detectar todos los dispositivos utilizados. Esto no creará reglas de control de acceso pero la organización, en función de su operativa, debe valorar esta opción.

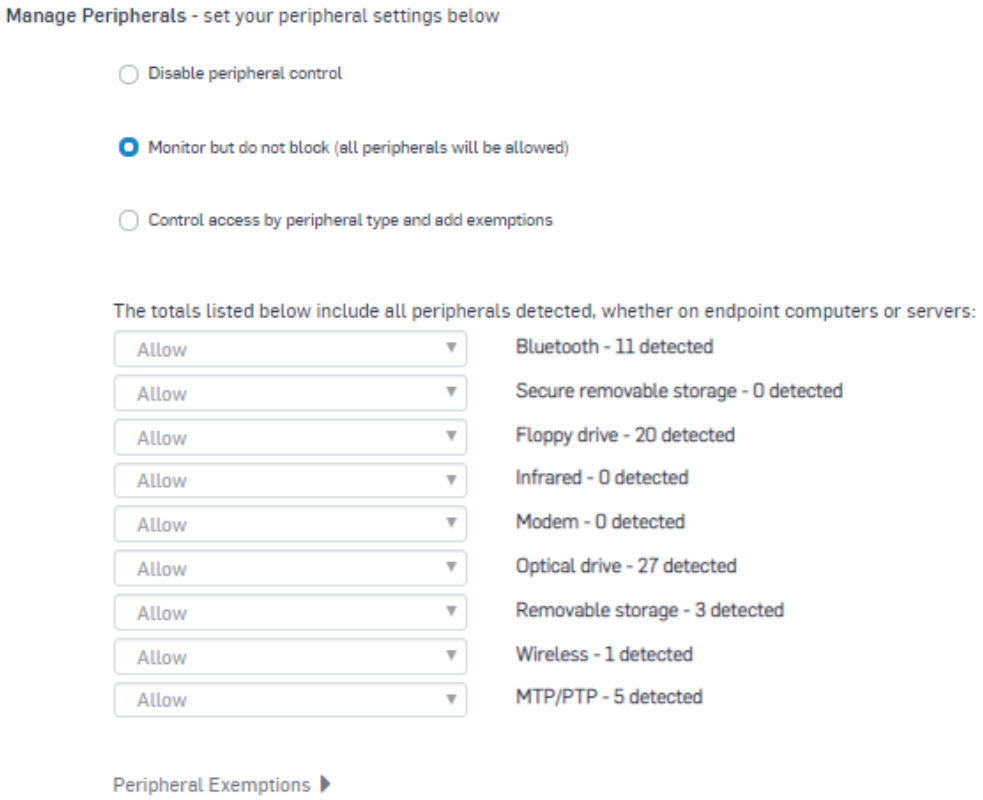

Ilustración 5-10. Activación del modo monitor

- El modo '*Control Access by peripheral type and add exemptions*' permite la creación de políticas de control de acceso para los dispositivos.

36. **Se debe realizar la siguiente configuración para la política de control de navegación (*Web Control Policy*).** Por defecto, el control de navegación de Sophos bloquea descargas potencialmente maliciosas (*.exe) así como el acceso a páginas de *proxies* y traductores (usados muchas veces como *proxies*). Será necesario revisar la política para ajustarla como mejor se adecue a las necesidades de la organización:

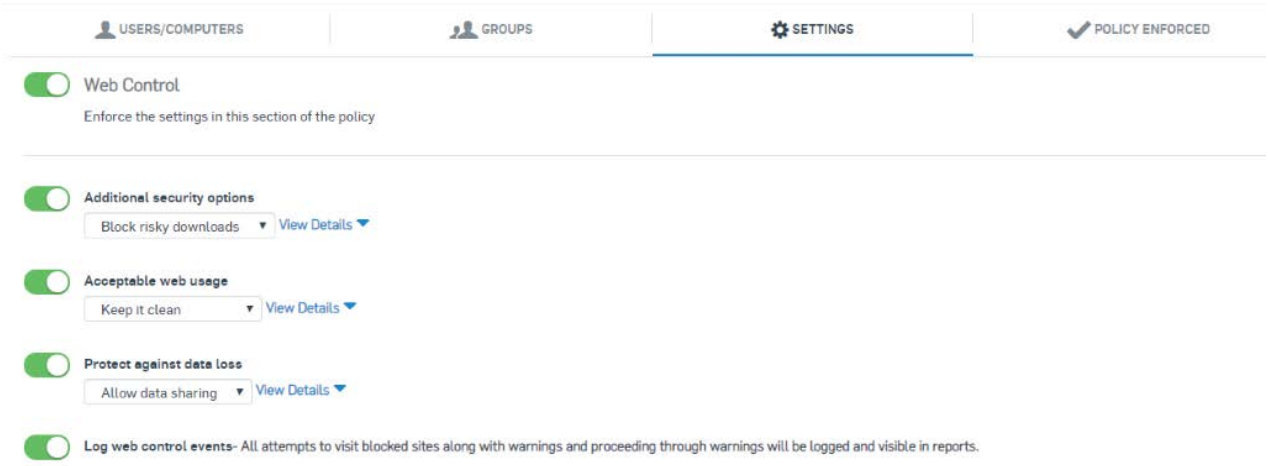

Ilustración 5-11. Edición de la política de acceso web

37. **Control de fuga de datos.** Permite definir qué ficheros debe salir de la organización. Esta debe definir qué datos se consideran sensibles y no deben salir al exterior de la red corporativa, bien por contenido o por tipo de fichero. Como "*best practice*" podría ser recomendable configurar una política de control, desde el correo electrónico y el navegador, de los ficheros más habituales, como son las hojas de cálculo, los documentos de texto, las presentaciones, etc. La política podría permita la salida de información pero implementar una monitorización exhaustiva de lo que sale del perímetro de la organización. La política define si se permite la transferencia, se bloquea o se deja la decisión al usuario en función de:

    - El contenido. Se pueden definir expresiones regulares (*regex*) para mirar dentro del fichero y decidir si se permite o no la transferencia.
    - El tipo de fichero. Se define si se permite o no la transferencia en función de si el fichero es una imagen, un video, un contenedor, presentaciones, etc. No se analiza el contenido del fichero.
    - El destino. Se establecen políticas en función de los posibles destinos: correo electrónico, navegador, mensajería, voz IP, almacenamiento, etc.

38. **Control de aplicaciones**. Permite definir si se quiere bloquear la ejecución de algún tipo de aplicación. Corresponde al administrador definir qué tipo de aplicaciones no quiere que se ejecuten en los equipos debido a que cada entorno tiene unos requisitos y características diferentes. Por defecto, no hay ninguna aplicación bloqueada.

39. Se recomienda la configuración de una política de control de aplicaciones para detectar aplicaciones tipo clientes FTP, complementos de navegador, gestores de descargas, P2P, juegos, mensajería instantánea, administración remota, telnet, etc. En resumen, **se deberán bloquear aquellas categorías de aplicaciones que pudieran constituir un riesgo de seguridad para la organización.**

40. En este artículo se detallan consejos de configuración:

    https://support.sophos.com/support/s/article/KB-000035468?language=en_US

41. **Control Firewall Windows**. Sophos puede controlar el *firewall* de Windows. Se puede habilitar, bloquear todo el tráfico o bloquear todo con las exclusiones que lleguen por GPO desde el controlador de dominio.

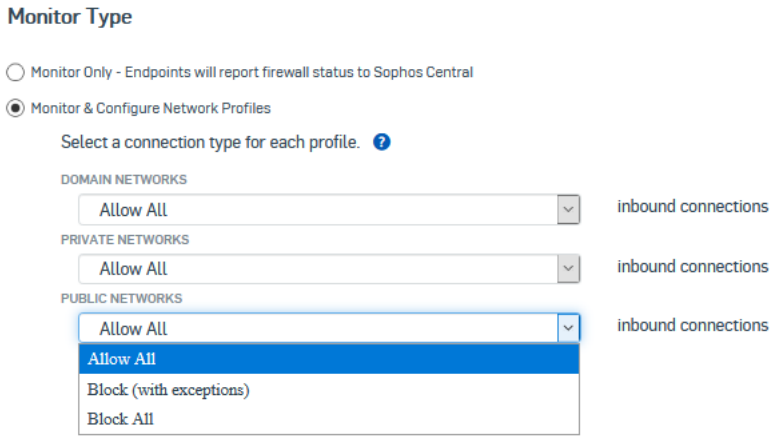

Ilustración 5-13. Configuración del *firewall* de Windows a través de Sophos

42. El detalle de la configuración de las distintas políticas se puede consultar en el apartado '*Policies*' de la guía *Sophos Central Admin Help* [REF1].

5.2 AUTENTICACIÓN

43. La autenticación en la plataforma de gestión Sophos Central se realiza mediante usuario y contraseña. Se pueden crear y gestionar usuarios (ver apartado 5.3.2 Gestión de usuarios), o se puede integrar con un servidor de directorio activo (ver apartado 5.4 Servidores de autenticación).

44. La complejidad de las contraseñas de usuario no es configurable. Por defecto, los parámetros de robustez de contraseñas que permite el producto son los siguientes:

    a) Longitud mínima de 8 caracteres (valor recomendado mínimo: 9 caracteres).

    b) Inclusión de mayúsculas y minúsculas.

    c) Inclusión de caracteres especiales.

    d) No utilización de una contraseña que sea la misma que la anterior.

45. Existen otros parámetros de robustez, de implementación procedimental, que deben ser tenidos en cuenta por los administradores:

    a) No usar palabras que puedan encontrarse en diccionarios

    b) No utilizar la repetición de, al menos, las 5 últimas contraseñas utilizadas.

    c) El valor recomendado para la vigencia y expiración de contraseñas no debe superar los 6 meses.

    d) No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio.

46. Dado que la política de contraseñas del producto no es suficientemente robusta, **se recomienda la utilización de autenticación multifactor en las cuentas de administración.** El producto permite configurar un código temporal de un solo uso (OTP) el cual puede ser obtenido mediante una aplicación tipo "*authenticator*" o mediante SMS.

47. Para configurar la autenticación Multi-factor (MFA) para los distintos usuarios, se deben seguir los siguientes pasos, desde una cuenta con **permisos de *SuperAdmin*** (ver 5.3.1 Configuración de administradores):

    - Ir a 'Global Settings'.
    - En el apartado General, hacer clic en *Multi-factor Authentication (MFA).*
    - Seleccionar una de las siguientes opciones:
        - *No MFA needed*. Los usuarios accederán a la consola de gestión haciendo uso solo de usuario/contraseña.
        - *All admins need MFA*. Todos los usuarios deberán configurar una de las opciones de códigos OTP disponibles.
        - *Select admins who will need MFA*. Permite seleccionar aquellos usuarios a los que se quiere añadir la autenticación MFA.
    - Se recomienda el uso del tercer método (*Select admins who will need MFA*), ya que, si fuera necesario desactivarlo para un administrador por algún motivo, se podría deshabilitar a dicho administrador únicamente y no a todas las cuentas de administrador.
    - Hacer clic en '*Save*'.

48. Cuando un usuario inicie sesión en la consola de gestión, tras haber sido habilitada la MFA en su cuenta, el producto mostrará una ventana indicando que debe configurarse la información adicional de autenticación.

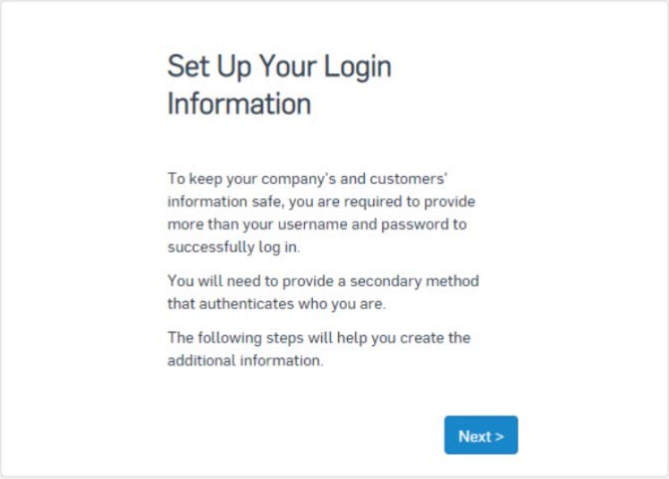

Ilustración 5-14. Configuración de autenticación multi-factor

49. El producto pedirá introducir un código enviado al mail del usuario, tras lo cual se permitirá selecciona la opción de MFA deseada.

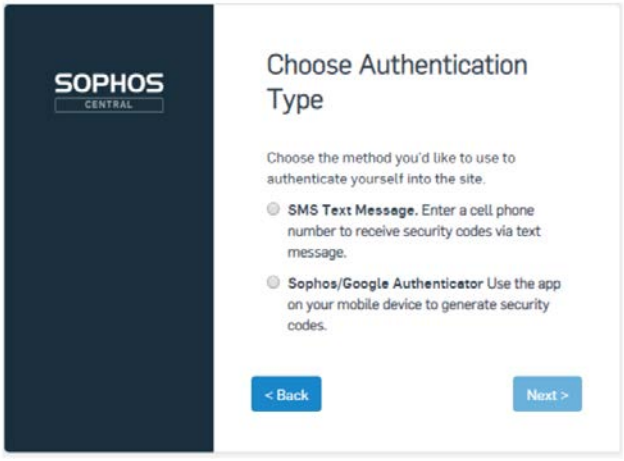

Ilustración 5-125. Selección del tipo de autenticación

50. En caso de seleccionar la opción de códigos mediante SMS, se deberá introducir el país y el número de teléfono. Finalmente se enviará un código a dicho número de teléfono para verificar que es correcto y finalizar la vinculación.

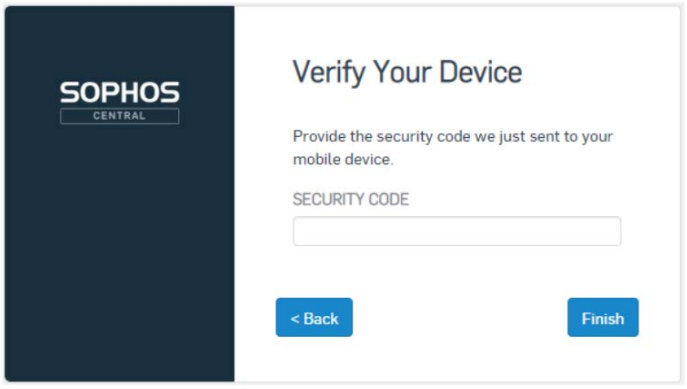

Ilustración 5-16. Verificación del dispositivo.

51. En caso de seleccionar la opción de utilizar *Authenticator*, se mostrará un código QR, que deberá escanearse con la aplicación para vincular el dispositivo, posteriormente se deberá introducir el código mostrado para finalizar la vinculación. Las posibles aplicaciones que pueden utilizarse para este método son *Sophos Authenticator* y *Google Authenticator*.

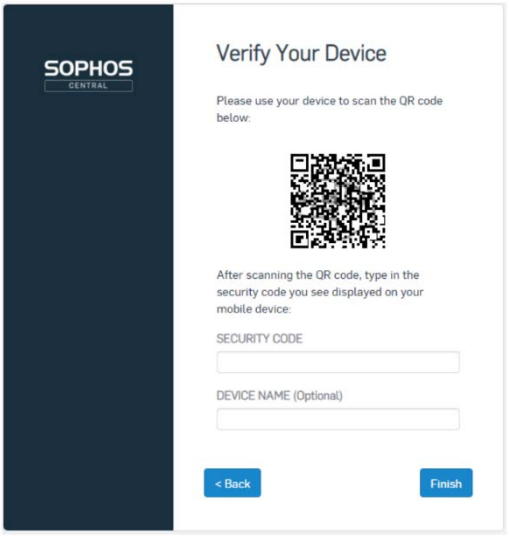

Ilustración 5-17. Verificación del dispositivo.

52. Una vez configurado el método deseado, en los posteriores inicios de sesión, se pedirá el código OTP adicional utilizando dicho método.

53. El detalle de la configuración de la autenticación Multi-factor se puede consultar en el apartado *Multi-factor authentication* de la guía *Sophos Central Admin Help* [REF1].

5.3 ADMINISTRACIÓN DEL PRODUCTO

54. La gestión del producto se realiza de forma remota, vía navegador web HTTPS a través del portal https://central.sophos.com.

5.3.1 CONFIGURACIÓN DE ADMINISTRADORES

55. El producto permite el RBAC (*Role Based Administration Control*) y, por defecto, tiene varios perfiles de administrador creados, los cuales no pueden modificarse ni eliminarse:

    - *SuperAdmin*: Permite realizar cualquier operación en la consola. Es el único rol con la capacidad gestionar y asignar roles.
    - *Admin*: Similar al rol *SuperAdmin*. Puede realizar cualquier operación, salvo crear/modificar roles y crear nuevos usuarios.
    - *HelpDesk*: Permite acceso en modo *Solo Lectura* a todos los ajustes en Sophos Central. Pueden realizar también las siguientes tareas:
        - Ver logs y reportes.
        - Recibir y solucionar alertas.
        - Actualizar el agente de un dispositivo.
        - Escanear dispositivos.

- *ReadOnly*: Similar al rol *HelpDesk*. Permite el acceso en modo *Solo Lectura* a todos los ajustes en Sophos Central. Pueden también realizar las siguientes tareas.
    - Ver logs y reportes.
    - Recibir alertas.

56. En cualquier caso, es posible añadir nuevos roles con los permisos que se deseen a partir de los roles ya existentes. Para esto:
    - Ir a Settings > Role Management > Add role.
    - Seleccionar el '*Base role*' a partir del cual se creará el nuevo rol.
    - Asignar un nombre y los permisos deseados al rol y hacer clic en '*Save*'.

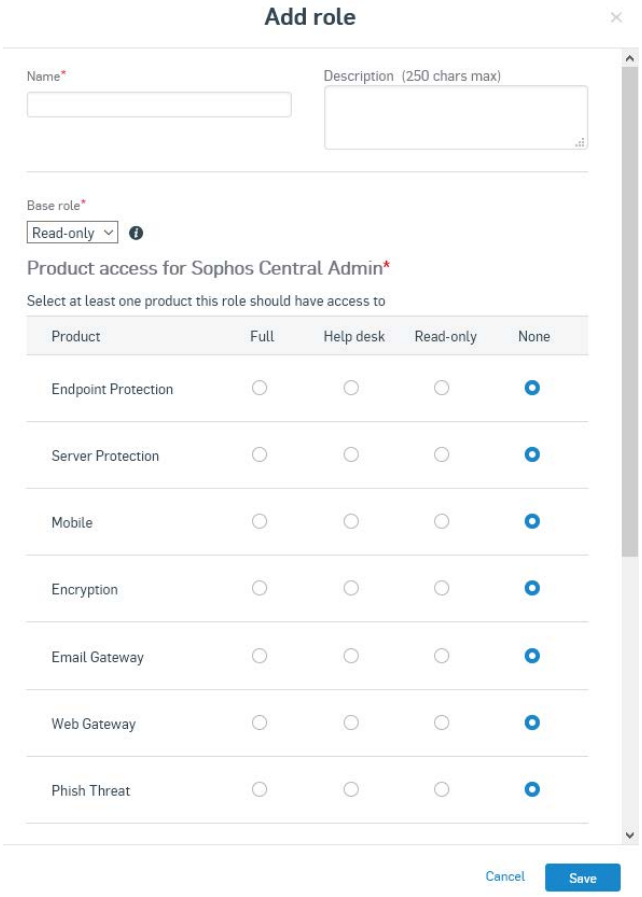

Ilustración 5-138. Configuración de roles

57. La consola permite la multiconcurrencia de administradores, por lo que es posible que un usuario con rol *Helpdesk* pueda estar trabajando mientras un usuario con rol *Admin* realiza cambios y otro con rol *ReadOnly* comprueba los logs. Esta característica no es configurable.
58. El detalle de la configuración de los roles de usuarios se puede consultar en el apartado *Role Management* de la guía *Sophos Central Admin Help* [REF1].

5.3.2 GESTIÓN DE USUARIOS

59. El producto permite la creación manual de usuarios:
    - Ir a Users > Add > Add User.
    - En el diálogo que aparecerá, introducir el nombre, rol y dirección de email.
    - Hacer clic en *Save*.
60. Adicionalmente, al ejecutar el instalador para proteger los dispositivos (ver apartado 4.5 Instalación) el producto crea automáticamente un usuario para cada dispositivo. Dicho usuario solo tendrá validez para poder asignar políticas y tendrá asignado el rol de "*user*".
61. Es posible modificar el rol de un usuario en cualquier momento siguiendo los siguientes pasos, desde una cuenta de usuario con permisos de *SuperAdmin*:
    - Ir a *Settings > Role Management* y seleccionar el rol que se quiere asignar.
    - En la página de detalles del rol, hacer clic en '*Edit*'.
    - Ir a '*Edit Role Members*' y seleccionar el usuario al que se desea asignar dicho rol de la lista que se muestra.
    - Finalmente hacer clic en *Save*.
62. Por defecto, todas las sesiones de cualquier rol de usuario caducan tras 30 minutos de inactividad. Esta opción no es configurable.
63. El detalle de la configuración de los usuarios se puede consultar en el apartado *Users* de la guía *Sophos Central Admin Help [REF1].*

5.4 SERVIDORES DE AUTENTICACIÓN

64. Es posible sincronizar un Servidor de Directorio Activo local para obtener el listado de usuarios y grupos. Para esto:
    - Ir a *Settings > Active Directory Sync*. Descargar el instalador de Sophos *Central AD Synchronization Utility Installer*. Tras la descarga, ejecutar el instalador.
    - Introducir la información requerida en el asistente de instalación. Al finalizar, seleccionar *Launch Sophos Central AD Sync Utility*.
    - En la página *AD Configuration*, introducir el servidor de directorio activo y las credenciales de un usuario con permisos de lectura. **Se debe mantener seleccionada la opción *'Use LDAP over an SSL connection'*, para realizar las comunicaciones mediante SSL.**

      La definición de qué versión de TLS utilizar depende del LDAP correspondiente. Sophos usara la que ya esté utilizando el LDAP**. Se debe utilizar la versión 1.2 de TLS o superior.**
    - La herramienta de Sophos AD Sync conecta con el LDAP de manera interna, de hecho la herramienta se puede instalar en el mismo server, aunque

puede instalarse en cualquier equipo de la red. Las comunicaciones hacia fuera serán como el resto, a través del puerto 443.

- En la página '*Sync Schedule*', especificar cada cuánto tiempo se realizará la sincronización automática.
- Hacer clic en '*Finish*'.

65. También es posible federar la autenticación a través de Azure AD para poder usar las mismas credenciales:
    - Ir a Settings > Federated Sign-in.
    - Seleccionar la forma de acceso de los usuarios. Si se selecciona '*Sign in with Microsoft credentials only*', los usuarios solo podrán acceder con las credenciales de Azure AD.
    - Se pueden añadir reglas específicas para usuarios concretos, permitiendo así que determinados usuarios accedan con las credenciales de Azure AD y con las credenciales de Sophos Central.
    - Hacer clic en '*Save*'.

5.5 ACTUALIZACIONES

66. El producto recibe diversos tipos de actualizaciones:
    - **Firmas**: depende del día y la actividad, pudiendo llegar a 20 al día, con tamaño promedio de 20KB.
    - Motores:
        - *AntiExploit* y *Deep Learning*: Cada 6 u 8 semanas recibe una actualización. Tamaño promedio: 30MB.
        - Motor AV: aproximadamente dos (2) veces por año. Tamaño promedio: 200MB.
67. Por defecto, los dispositivos reciben las actualizaciones de forma periódica y automática. El producto comprueba cada 10 minutos si se encuentran actualizaciones disponibles. Las actualizaciones de motores se pueden programar, las de firmas no.
68. Para programar las actualizaciones, es necesario crear una *Updating Policy*. Para esto, ir a *Policies* > *Updating Policy* e introducir los días y horas en los que se desea que se realicen las actualizaciones (en caso de haber actualizaciones disponibles).

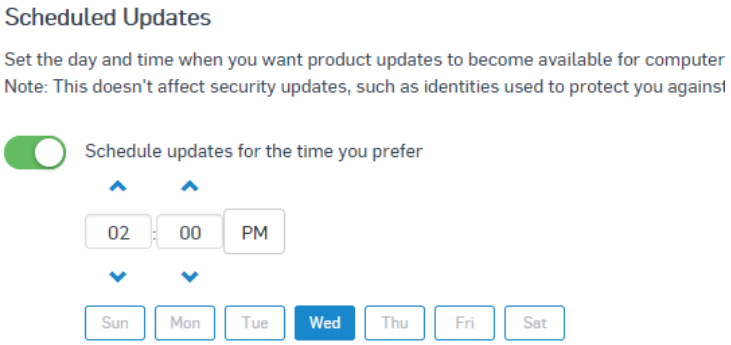

Ilustración 5-149. Programación de actualizaciones

69. En caso de haber configurado *Update Caches* y *Message Relays*, los dispositivos obtendrán las actualizaciones de estos, por lo que será necesario haber configurado correctamente las comunicaciones desde dichos componentes hacia los servicios de Sophos, según lo indicado en el apartado 4.4 Consideraciones previas.

70. En caso de no haber configurado dichos componentes, todos los dispositivos deberán contar con acceso a los servicios de Sophos para poder obtener las actualizaciones de forma correcta.

5.5.1 SEGURIDAD EN LAS ACTUALIZACIONES

71. Por defecto, el producto obtiene las actualizaciones mediante el protocolo HTTPS. **Se debe verificar que se encuentra habilitado el uso de HTTPS** seguir los siguientes pasos:

    - Ir a Settings > HTTPS Updating.
    - Verificar que *HTTPS Updating* se encuentra activado.

72. La activación de *HTTPS Updating* afecta a las siguientes comunicaciones, haciendo obligatorio el uso de HTTPS:

    - Descarga de las actualizaciones desde Sophos Central por los dispositivos o por los *Update Caches*.
    - Obtención de las actualizaciones desde los *Update Caches* por los dispositivos.

5.6 GESTIÓN DE CERTIFICADOS

73. El producto hace uso de certificados en las comunicaciones HTTPS entre los dispositivos y los *Update Caches*, así como entre Sophos Central y los dispositivos/*Update Caches*, para la obtención y distribución de las actualizaciones. Dichos certificados no son configurables y en caso de no detectarse el certificado de Sophos en alguna comunicación, esta no se inicia.

5.7 AUTO-CHEQUEOS

74. El producto de forma automática y continuada realiza una evaluación de su configuración y, en caso de detectar un servicio caído o en un estado incorrecto, tratará de corregirlo. Si tras varios intentos sigue sin poder resolver la situación, entrará en modo de auto-reparación, donde el producto se reinstala de forma silenciosa y automática.

75. En este caso, las configuraciones que ya estuvieran establecidas se vuelven a asignar de manera automática, dependiendo de la máquina o usuario loguedado. No es necesario realizar ninguna acción para que la maquina reinstalada se configure.

76. El objetivo era garantizar que el producto está siempre en perfecto estado y con su auto-reparación minimizar la necesidad de soporte.

5.8 AUDITORÍA

5.8.1 REGISTRO DE EVENTOS

77. Sophos Central dispone de dos (2) tipos de logs:

- **Eventos**: se registran todos los eventos relacionados con el producto. Como detecciones, incidentes, etc. Todo ello almacenado en la nube por 90 días, independientemente del número de eventos. El periodo de retención en la nube no es configurable.

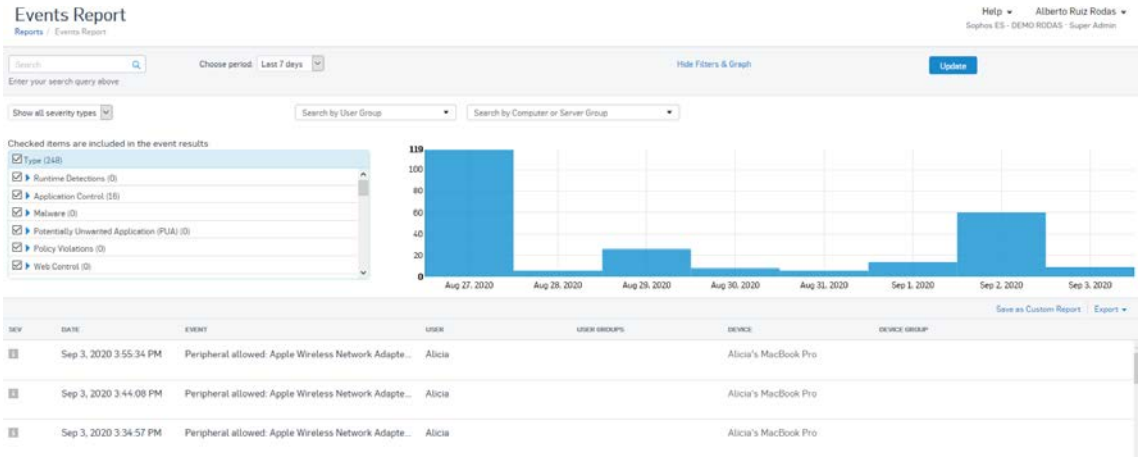

Ilustración 5-20. Registro de eventos.

- **Auditoría**: cambios realizados en la configuración: quién lo ha hecho, sobre qué, etc… Todo ello se almacena en la nube por 90 días, independientemente del número de eventos. El periodo de retención en la nube no es configurable.

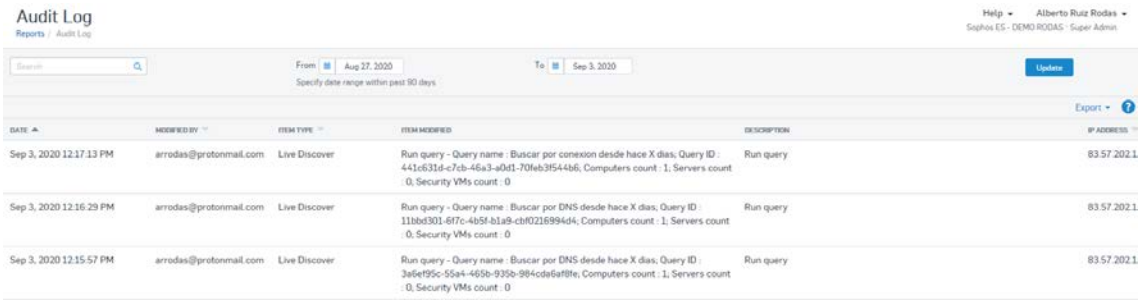

Ilustración 5-21. Registro de logs de auditoría.

78. Se dispone además de RCA (*Root Cause Analsys*) en los que aparecerá detallado el motivo de qué ha sucedido:

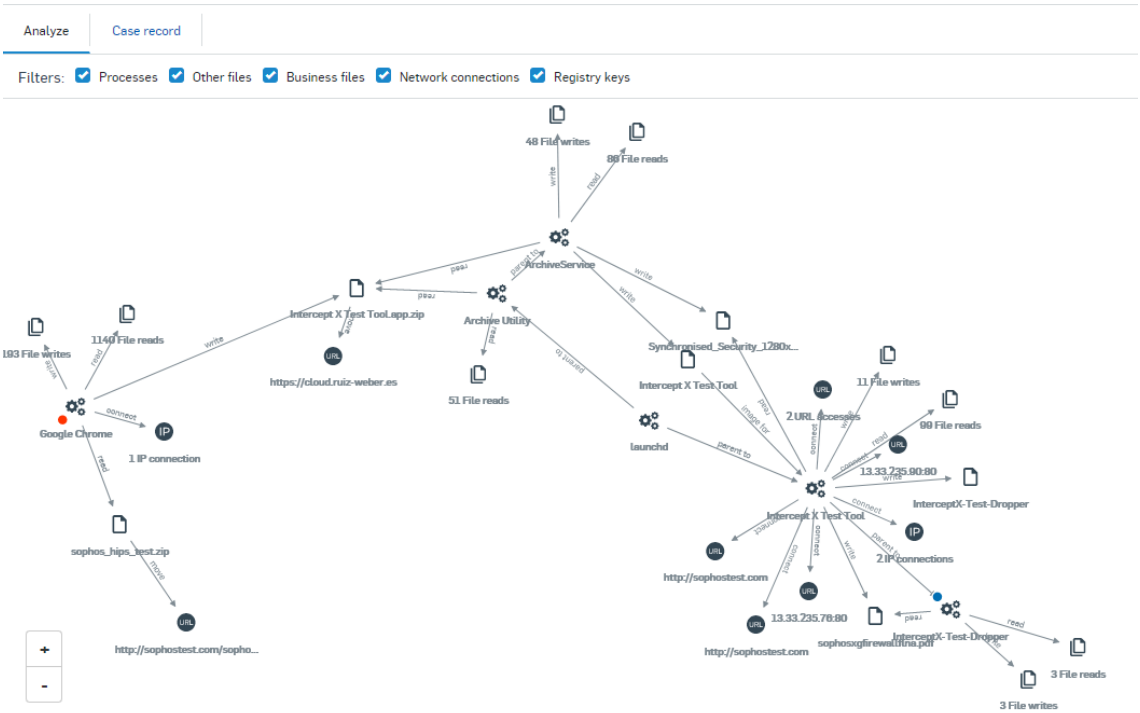

Ilustración 5-22. Detalle de información de logs

79. Es posible exportar dicho grafo a un formato de base de datos relacional para, por ejemplo, realizar búsquedas y obtener así información aún más detallada.

80. Finalmente, si se dispone de EDR, es posible realizar acciones de búsqueda para casi cualquier tipo de evento. Por ejemplo, si un grupo de equipos ha intentado resolver el DNS www.sophos.com hace 47 días, se puede saber qué proceso lo ha hecho, con qué usuario, etc. Es lo que se denomina *Live Discover* y permite la consulta de tablas almacenadas en los propios equipos en tiempo real, permitiendo un histórico de hasta 90 días. El periodo de retención en la nube no es configurable. El detalle de tablas que se pueden consultar está en:

https://support.sophos.com/support/s/article/KB-000038469?language=en_US

https://osquery.io/schema/4.2.0

5.8.2 ALMACENAMIENTO LOCAL

81. Es posible realizar un almacenamiento local de los eventos mediante el uso de una API que permite el reenvío de los eventos a un servidor de auditoría Syslog o bien a un sistema SIEM. Todas las comunicaciones de Sophos se realizan a través de TLS 1.2, con intercambio de claves ECDHE_RSA y cifrado AES_128_GCM. Esta configuración no es parametrizable.

82. Para más detalles sobre cómo realizar dicha integración, se recomienda ver: https://community.sophos.com/kb/en-us/125169

5.8.3 ALMACENAMIENTO REMOTO

83. El almacenamiento remoto de los logs se realiza de forma automática en la nube de Sophos. Estos datos son accesibles desde la consola de gestión, desde la página *Logs & Reports*.

84. Adicionalmente, es posible exportar los logs de auditoría del producto desde la consola de gestión, para posteriormente almacenarlos en la ubicación deseada:

    - Ir a '*Logs & Reports*' y seleccionar '*Audit Logs'*.
    - Hacer clic en '*Export',* a la derecha de la página *'Audit Log'* y seleccionar una de las opciones:
        - *CSV of current view* o *PDF of current view*. Esta opción exporta, en el formato elegido, los logs de auditoría de la vista actual.
        - *CSV of past 90 days* o *PDF of past 90 days*. Esta opción exporta en el formato elegido, todos los logs de auditoría de los últimos 90 días

6. FASE DE OPERACIÓN

85. La operativa habitual de este producto consistirá en, de forma periódica:

- Revisar las alertas. Éstas están ordenadas por criticidad: alta, media, baja
- Resolver lo antes posible las alertas de criticidad ALTA, siguiendo con las de MEDIA y finalmente las de BAJA.
- Realizar la exportación de logs y enviar a un SIEM o Syslog.
- En caso de tener una detección, revisar el para comprobar el verdadero origen de la amenaza.
- Si se dispone de EDR, realizar búsquedas periódicas para detectar acciones "extrañas", conexiones "extrañas", etc… Si se dispone de EDR, gracias a los "*Threat Indicators*", analizar aquellos binarios que, si bien no ha lanzado una detección (firmas, *Deep Learning*, *exploits*, etc…), se consideran sospechosos y enviar a un centro de *sandboxing* para su análisis en profundidad. Tanto el análisis de RCA, como los detalles de EDR permitirán realizar una limpieza preventiva del binario que, si bien no ha detonado una amenaza, tras los pasos de análisis se descubre sospechoso e inadecuado, pudiendo de forma centralizada realizar la limpieza global.
- Verificar que el producto está correctamente actualizado, tanto las firmas como los motores.
- Verificar que los administradores disponen de MFA, de acuerdo a las políticas establecidas en la organización.
- Verificar que el modo de operación seguro sigue operativo de acuerdo a su configuración inicial.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la firma del instalador	☐	☐	
Instalación en un entorno seguro, con *Update Cache* y un *Message Relay*	☐	☐	
Registro de las licencias	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de operación seguro activado según recomendaciones	☐	☐	
Revisión políticas de prevención de amenazas	☐	☐	
Revisión de políticas de control de dispositivos	☐	☐	
Revisión de políticas de control de navegación	☐	☐	
Revisión de políticas de firewall de Windows	☐	☐	
Revisión de políticas de control de aplicaciones	☐	☐	
Revisión de políticas de control de fuga de datos	☐	☐	
Activación de la autenticación Multi-Factor	☐	☐	

8. REFERENCIAS

[REF1] *Sophos Central Admin Help*
https://docs.sophos.com/central/Customer/help/en-us/PDF/sc_customer_h.pdf

9. ABREVIATURAS

AD	*Active Directory*
CPU	*Central Processing Unit*
EDR	*Endpoint Detection and Response*
ENS	*Esquema Nacional de Seguridad.*
HTTPS	*Hyper Text Transfer Protocol Secure*
LDAP	*Lightweight Directory Access Protocol*
MFA	*Multi Factor Authentication*
OTP	*One Time Password*
RBAC	*Role Based Access Control*
RCA	*Root Cause Analisys*
SMS	*Short Message Service*
TCP	*Transmission Control Protocol*