

maestre
corporación

Informe de configuración Endpoint SOPHOS CENTRAL

ALCANCE

Dar a conocer las configuraciones realizadas en la consola de Sophos Central del **Alcaldía de Mosquera**, según los acuerdos del proyecto, a fin de brindar la protección adecuada a las estaciones de trabajo y servidores de la organización.

CLIENTE

Cliente

Alcaldía de Mosquera

Producto

Intercept X Advanced with XDR

LICENCIA ACTUAL

El **Alcaldía de Mosquera** dispone de un límite de 470 (cuatrocientos setenta) licencias de Intercept X Advanced with XDR para estaciones de trabajo, de las cuales 334 (trescientos treinta y cuatro) están actualmente en uso.

Partner: Corporación Maestre SAS

SOPHOS

Paneles de control

Mis productos

Centro de análisis de amenazas

Alertas

Informes

Más

Alcaldía de Mosquera

Licencias

Ver información de licencia y uso

Licencias del producto

Licencias de firewall

Detalles de la licencia

Última actualización: 23 nov. 2023, 11:32

Aplicar clave de licencia

Contactar con partner para comprar

Licencia	Tipo	Uso	Límite	Comienza	Vence	Licencia #
Intercept X Advanced with XDR	Completa	334	470	28 de sep. de 2023	27 de sep. de 2024	MGR00003507

Leer Acuerdo de licencia de usuario final

Adquirir Sophos Central Protection

Puede adquirir Sophos Central a través de un distribuidor autorizado.



Endpoint



Políticas del Computador

Endpoint Protection - Políticas

Alcaldía de Mosquera

Introducción / Panel de control de Endpoint Protection / Políticas

Buscar

Añadir política

Eliminar

Nota: Las políticas del principio de la lista anulan las políticas del final de la lista.

Protección contra amenazas (3)				
?	Nombre	Estado	Tipo (individual / grupo)	Última actualización
⋮	Exploit prevented in Microsoft Office	✓ Impuestas	Ordenador (0 / 0)	16 oct. 2023
⋮	Política Principal - Threat Protection	✓ Impuestas	Ordenador (1 / 0)	18 oct. 2023
	Política base - Protección contra amenazas	✓ Impuestas		21 nov. 2023
Control de periféricos (3)				
?	Nombre	Estado	Tipo (individual / grupo)	Última actualización
⋮	BIBLIOTECA	Ignoradas	Usuario (0 / 0)	22 nov. 2023
⋮	Política Principal - Peripheral Control	✓ Impuestas	Ordenador (1 / 0)	18 oct. 2023
	Política base - Control de periféricos	✓ Impuestas		18 oct. 2023
Restricción de aplicaciones (3)				
?	Nombre	Estado	Tipo (individual / grupo)	Última actualización
⋮	Política Personalizada - Application Control	Ignoradas	Ordenador (0 / 0)	20 oct. 2023
⋮	Política Principal - Application Control	✓ Impuestas	Ordenador (1 / 0)	18 oct. 2023
	Política base - Restricción de aplicaciones	✓ Impuestas		24 oct. 2023
Prevención de pérdida de datos (2)				
	Nombre	Estado	Tipo (individual / grupo)	Última actualización
	Política Principal - Data Loss Prevention	✓ Impuestas	Ordenador (1 / 0)	9 jun. 2023
	Política base - Prevención de pérdida de datos	✓ Impuestas		9 jun. 2023
Control web (3)				
?	Nombre	Estado	Tipo (individual / grupo)	Última actualización
⋮	CAD	✓ Impuestas	Usuario (0 / 1)	22 nov. 2023
⋮	Política Principal - Web Control	Ignoradas	Usuario (4 / 0)	20 oct. 2023
	Política base - Control web	✓ Impuestas		27 oct. 2023
Gestión de actualizaciones (1)				
	Nombre	Estado	Tipo (individual / grupo)	Última actualización
	Política base - Gestión de actualizaciones	✓ Impuestas		9 jun. 2023
Firewall de Windows (1)				
	Nombre	Estado	Tipo (individual / grupo)	Última actualización
	Política base - Firewall de Windows	✓ Impuestas		9 jun. 2023



Protección contra amenazas (Threat Protection) - Exploit prevented in Microsoft Office:

Endpoint Protection - Ver política de ordenadores

Introducción / Políticas de ordenador / Ver política de ordenador

Alcaldía de Mosquera

NOMBRE DE POLÍTICA* Exploit prevented in Microsoft Office

Guardar Cancelar Eliminar Clonar

TIPO DE POLÍTICA Protección contra amenazas : Dispositivo

Última actualización 16 oct. 2023

0 ORDENADORES 0 GRUPOS CONFIGURACIÓN POLÍTICA IMPUESTA

Sus configuraciones de políticas le ofrecen la protección que recomendamos.

Live Protection

- Use Live Protection para comprobar la información sobre amenazas más reciente de SophosLabs online
 - Usar Live Protection durante los escaneados programados
- Nota: Es posible que los datos salgan de su región geográfica y se compartan con los ingenieros de Sophos.

Se aplica a



Deep Learning

- Activar Deep Learning



Escaneo en tiempo real - Archivos locales y recursos de red

- Activar escaneo en tiempo real
 - Archivos remotos



Escaneo en tiempo real - Internet

- Escanear descargas en progreso
- Bloquear el acceso a sitios web maliciosos
- Detectar archivos de baja reputación



Remediación

- Limpiar malware automáticamente. Consulte la [help](#) para conocer las excepciones.
- Activar creación de gráfico de amenazas



Protección en tiempo de ejecución

- Proteger archivos de documentos de ransomware (CryptoGuard)
 - Proteger de ransomware ejecutado de forma remota
 - Protegerse de ataques de cifrado del sistema de archivos



Protección contra amenazas (Threat Protection) - Exploit prevented in Microsoft Office:

Impedir que cargas maliciosas se conecten a servidores de comando y control

Nuevo: Los clientes obtendrán esta función gradualmente a medida que los equipos se actualicen a la última versión de Sophos Intercept X

Proteger el tráfico de red

✓ Detectar conexiones maliciosas con servidores de comando y control

☐ Impedir el tráfico de red malicioso con la inspección de paquetes (IPS)

ⓘ Nota:

Solo se aplica a los dispositivos que añada al EAP de Nuevas funciones de Endpoint Protection. Eliminaremos este ajuste pronto.

Detectar comportamiento malicioso

Nuevo: Los clientes obtendrán esta función gradualmente a medida que los equipos se actualicen a la última versión de Core Agent

✓ Protección contra adversarios activos adaptativa

☒ Si está desactivada, los comportamientos de adversarios activos se notifican en Detecciones para los clientes de XDR

Protección AMSI (con escaneado mejorado para las amenazas basadas en scripts)

Impedir eliminación del registro de AMSI

Se aplica a

Configuración avanzada

Recomendamos que mantenga las opciones predeterminadas. Sin embargo, puede resultarle útil cambiarlas de forma temporal. [Más información](#)

Ver configuración avanzada

✓ Activar la protección antiransomware y todas las mitigaciones de exploits

?

✓ Activar todos los enlaces de mitigaciones de exploits

✓ Escanear instaladores de confianza

✓ Utilizar el escaneado recomendado de adjuntos de correo electrónico

Nivel de detección de Deep Learning: Predeterminado

✓ Realizar seguimiento de las conexiones de red

✓ Activar el registro de eventos

✓ Generar hashes de archivo de forma remota para el registro de eventos

✓ Escanear periódicamente la memoria del proceso en segundo plano

Se aplica a

Descifrado SSL/TLS de sitios web HTTPS

☐ Descifrar sitios web HTTPS usando SSL/TLS. Si se activa, también se activa el descifrado HTTPS para el control web

ⓘ Este ajuste se aplica a todos los dispositivos Windows. También se aplica a los equipos Mac que añada al EAP de nuevas funciones de Endpoint Protection para macOS

ⓘ Puede excluir sitios web del descifrado en las páginas de ajustes globales

Aislamiento de dispositivo

☐ Permitir a los ordenadores autoaislarse cuando su estado de seguridad está en rojo

ⓘ Nota:

Si el estado de seguridad de un ordenador está en rojo, se autoaislará de la red. Aunque seguirá comunicándose con Sophos Central.

Escaneo programado

☒ Activar escaneo programado

11:30 AM

dom.

lun.

mar.

mié.

jue.

vie.

sáb.

☐ Activar escaneo profundo - escanea dentro de archivos comprimidos (.zip, .cab, etc.)

Se aplica a

Exclusiones

Ver exclusiones globales

Exclusiones de políticas

Excluir

Activo para

Excluir Microsoft Access de la comprobación

Mitigación de exploits (Windows)

X

30b7088bfbac18444d651fd718596eb411a571477c06ad379dd0d879db1ad5d2

Proceso (Windows)

X

Mensaje de escritorio

☒ Activar los mensajes de escritorio para la protección contra amenazas

Configurar un mensaje para añadirlo al final de la notificación estándar

ⓘ Nota:

Los mensajes personalizados no se mostrarán para eventos Intercept X

Se aplica a



Protección contra amenazas (Threat Protection) - Política Principal - Threat Protection:

Endpoint Protection - Ver política de ordenadores

Alcaldía de Mosquera

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA*

Política Principal - Threat Protection

Guardar

Cancelar

Eliminar

Clonar

TIPO DE POLÍTICA

Protección contra amenazas : Dispositivo

Última actualización

18 oct. 2023

1 ORDENADORES

0 GRUPOS

CONFIGURACIÓN

POLÍTICA IMPUESTA

Sus configuraciones de políticas le ofrecen la protección que recomendamos.

Live Protection

Se aplica a

Windows

Mac

Use Live Protection para comprobar la información sobre amenazas más reciente de SophosLabs online

Usar Live Protection durante los escaneos programados

Nota: Es posible que los datos salgan de su región geográfica y se compartan con los ingenieros de Sophos.

Deep Learning

Activar Deep Learning

Escaneado en tiempo real - Archivos locales y recursos de red

Activar escaneado en tiempo real

Archivos remotos

Escaneado en tiempo real - Internet

Escanear descargas en progreso

Bloquear el acceso a sitios web maliciosos

Detectar archivos de baja reputación

ACCIÓN PARA DESCARGAS DE BAJA REPUTACIÓN

Preguntar

NIVEL DE REPUTACIÓN

Recomendado

Remediación

Limpiar malware automáticamente. Consulte la help para conocer las excepciones.

Activar creación de gráfico de amenazas

Protección en tiempo de ejecución

Proteger archivos de documentos de ransomware (CryptoGuard)

Proteger de ransomware ejecutado de forma remota

Protegerse de ataques de cifrado del sistema de archivos

ACCIÓN PARA REALIZAR AL DETECTAR RANSOMWARE

Finalizar proceso

Proteger contra el ransomware de registro de arranque maestro

Proteger funciones críticas en navegadores web (Navegación segura)

Mitigar vulnerabilidades en aplicaciones vulnerables

Proteger navegadores web

Proteger complementos de navegadores web

Proteger aplicaciones Java

Proteger aplicaciones multimedia

Proteger aplicaciones de oficina

Proteger procesos

Impedir ataques de vaciado de procesos

Impedir que se carguen archivos DLL de carpetas de no confianza

Impedir el robo de credenciales

Impedir el robo de credenciales del registro

Impedir el uso de cuevas de código

Impedir la infracción de APC

Impedir el aumento de privilegios

Protección shellcode dinámica

Validar invocador del protocolo CTF

Impedir la carga lateral de módulos no seguros

Nuevo: Los clientes obtendrán esta función gradualmente a medida que los equipos se actualicen a la última versión de Sophos Intercept X

Proteger las cookies del navegador utilizadas para el inicio de sesión con MFA

Nueva



Protección contra amenazas (Threat Protection) - Política Principal - Threat Protection:

Nuevo: Los clientes obtendrán esta función gradualmente a medida que los equipos se actualicen a la última versión de Sophos Intercept X

Impedir que cargas maliciosas se conecten a servidores de comando y control **Nueva**

Nuevo: Los clientes obtendrán esta función gradualmente a medida que los equipos se actualicen a la última versión de Sophos Intercept X

Proteger el tráfico de red

✓ Detectar conexiones maliciosas con servidores de comando y control

✗ Impedir el tráfico de red malicioso con la inspección de paquetes (IPS)

Nota: Solo se aplica a los dispositivos que añade al EAP de Nuevas funciones de Endpoint Protection. Eliminaremos este ajuste pronto.

Detectar comportamiento malicioso **Nueva**

Nuevo: Los clientes obtendrán esta función gradualmente a medida que los equipos se actualicen a la última versión de Core Agent

✓ Protección contra adversarios activos adaptativa

✗ Si está desactivada, los comportamientos de adversarios activos se notifican en Detecciones para los clientes de XDR

Protección AMSI (con escaneo mejorado para las amenazas basadas en scripts)

Impedir eliminación del registro de AMSI

Configuración avanzada

Recomendamos que mantenga las opciones predeterminadas. Sin embargo, puede resultarle útil cambiarlas de forma temporal. [Más información](#)

Ver configuración avanzada

✓ Activar la protección antirransomware y todas las mitigaciones de exploits ?

✓ Activar todos los enlaces de mitigaciones de exploits

✓ Escanear instaladores de confianza

✓ Utilizar el escaneo recomendado de adjuntos de correo electrónico

Nivel de detección de Deep Learning:

Predeterminado

✓ Realizar seguimiento de las conexiones de red

✓ Activar el registro de eventos

✓ Generar hashes de archivo de forma remota para el registro de eventos

✓ Escanear periódicamente la memoria del proceso en segundo plano

Se aplica a

Descifrado SSL/TLS de sitios web HTTPS

Descifrar sitios web HTTPS usando SSL/TLS. Si se activa, también se activa el descifrado HTTPS para el control web

Este ajuste se aplica a todos los dispositivos Windows. También se aplica a los equipos Mac que añada al EAP de nuevas funciones de Endpoint Protection para macOS

Puede excluir sitios web del descifrado en las [páginas de ajustes globales](#)

Aislamiento de dispositivo

Permitir a los ordenadores autoaislarse cuando su estado de seguridad está en rojo

Nota: Si el estado de seguridad de un ordenador está en rojo, se autoislará de la red. Aunque seguirá comunicándose con Sophos Central.

Escaneo programado

Activar escaneo programado

11:30 AM

dom.

lun.

mar.

mié.

jue.

vie.

sáb.

Activar escaneo profundo - escanea dentro de archivos comprimidos (.zip, .cab, etc.)

Exclusiones

Ver exclusiones globales ?

Exclusiones de políticas

Añadir exclusión

Excluir

Activo para

Actualmente no hay exclusiones

Mensaje de escritorio

Activar los mensajes de escritorio para la protección contra amenazas

Configurar un mensaje para añadirlo al final de la notificación estándar

Nota: Los mensajes personalizados no se mostrarán para eventos Intercept X



Protección contra amenazas (Threat Protection) - Política base - Protección contra amenazas:

Endpoint Protection - Ver política de ordenadores

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA: Política base - Protección contra amenazas

GuardarCancelarClonarRestablecer

TIPO DE POLÍTICA: Protección contra amenazas : Usuario

Última actualización: 21 nov. 2023

USUARIOS/ORDENADORESGRUPOSCONFIGURACIÓNPOLÍTICA IMPUESTA

Sus configuraciones de políticas le ofrecen la protección que recomendamos.

Live Protection

Se aplica a

WindowsMac

Use Live Protection para comprobar la información sobre amenazas más reciente de SophosLabs online

Usar Live Protection durante los escaneados programados

Nota: Es posible que los datos salgan de su región geográfica y se compartan con los ingenieros de Sophos.

Deep Learning

Activar Deep Learning

Escaneado en tiempo real - Archivos locales y recursos de red

Activar escaneado en tiempo real

Archivos remotos

Escaneado en tiempo real - Internet

Escanear descargas en progreso

Bloquear el acceso a sitios web maliciosos

Detectar archivos de baja reputación

Acción para descargas de baja reputación

Preguntar

Nivel de reputación

Recomendado

Introducción / Políticas de ordenador / Ver política de ordenador

Alcaldía de Mosquera

Remediación

Limpiar malware automáticamente. Consulte la help para conocer las excepciones.

Activar creación de gráfico de amenazas

Protección en tiempo de ejecución

Proteger archivos de documentos de ransomware (CryptoGuard)

Proteger de ransomware ejecutado de forma remota

Protegerse de ataques de cifrado del sistema de archivos

Acción para realizar al detectar ransomware

Finalizar proceso

Proteger contra el ransomware de registro de arranque maestro

Proteger funciones críticas en navegadores web (Navegación segura)

Mitigar vulnerabilidades en aplicaciones vulnerables

Proteger navegadores web

Proteger complementos de navegadores web

Proteger aplicaciones Java

Proteger aplicaciones multimedia

Proteger aplicaciones de oficina

Proteger procesos

Impedir ataques de vaciado de procesos

Impedir que se carguen archivos DLL de carpetas de no confianza

Impedir el robo de credenciales

Impedir el robo de credenciales del registro

Impedir el uso de cuevas de código

Impedir la infracción de APC

Impedir el aumento de privilegios

Protección shellcode dinámica

Validar invocador del protocolo CTF

Impedir la carga lateral de módulos no seguros Nueva

Nuevo: Los clientes obtendrán esta función gradualmente a medida que los equipos se actualicen a la última versión de Sophos Intercept X

Proteger las cookies del navegador utilizadas para el inicio de sesión con MFA Nueva

NIT: 901161495-0
BOGOTÁ AV. CARRERA 15 #119-11. OFICINA 502

Protección contra amenazas (Threat Protection) - Política base - Protección contra amenazas:

Nuevo: Los clientes obtendrán esta función gradualmente a medida que los equipos se actualicen a la última versión de Sophos Intercept X

Impedir que cargas maliciosas se conecten a servidores de comando y control **Nueva**

Nuevo: Los clientes obtendrán esta función gradualmente a medida que los equipos se actualicen a la última versión de Sophos Intercept X

Proteger el tráfico de red

✓ Detectar conexiones maliciosas con servidores de comando y control

✓ Impedir el tráfico de red malicioso con la inspección de paquetes (IPS)

ⓘ Nota: Solo se aplica a los dispositivos que añada al EAP de Nuevas funciones de Endpoint Protection. Eliminaremos este ajuste pronto.

Detectar comportamiento malicioso **Nueva**

Nuevo: Los clientes obtendrán esta función gradualmente a medida que los equipos se actualicen a la última versión de Core Agent

✓ Protección contra adversarios activos adaptativa

■ Si está desactivada, los comportamientos de adversarios activos se notifican en Detecciones para los clientes de XDR

Protección AMSI (con escaneado mejorado para las amenazas basadas en scripts)

Impedir eliminación del registro de AMSI

Se aplica a

Se aplica a

Configuración avanzada

Recomendamos que mantenga las opciones predeterminadas. Sin embargo, puede resultarle útil cambiarlas de forma temporal. [Más información](#)

Ver configuración avanzada

✓ Activar la protección antirransomware y todas las mitigaciones de exploits ⓘ

✓ Activar todos los enlaces de mitigaciones de exploits

✓ Escanear instaladores de confianza

✓ Utilizar el escaneado recomendado de adjuntos de correo electrónico

Nivel de detección de Deep Learning: Predeterminado

✓ Realizar seguimiento de las conexiones de red

✓ Activar el registro de eventos

✓ Generar hashes de archivo de forma remota para el registro de eventos

✓ Escanear periódicamente la memoria del proceso en segundo plano

Se aplica a

Descifrado SSL/TLS de sitios web HTTPS

Descifrar sitios web HTTPS usando SSL/TLS. Si se activa, también se activa el descifrado HTTPS para el control web

ⓘ Este ajuste se aplica a todos los dispositivos Windows. También se aplica a los equipos Mac que añada al EAP de nuevas funciones de Endpoint Protection para macOS

ⓘ Puede excluir sitios web del descifrado en las [páginas de ajustes globales](#)

Aislamiento de dispositivo

Permitir a los ordenadores autoaislarse cuando su estado de seguridad está en rojo

ⓘ Nota: Si el estado de seguridad de un ordenador está en rojo, se autoaislará de la red. Aunque seguirá comunicándose con Sophos Central.

Escaneo programado

Activar escaneo programado

12:00 PM

dom.

lun.

mar.

mié.

jue.

vie.

sáb.

☐ Activar escaneo profundo - escanea dentro de archivos comprimidos (.zip, .cab, etc.)

Se aplica a

Exclusiones

Ver exclusiones globales ⓘ

Exclusiones de políticas

Añadir exclusión

Excluir

C:\Servidor\650b
Archivo o carpeta (Windows)

Activo para

En tiempo real y programado

X

Mensaje de escritorio

Activar los mensajes de escritorio para la protección contra amenazas

Configurar un mensaje para añadirlo al final de la notificación estándar

ⓘ Nota: Los mensajes personalizados no se mostrarán para eventos Intercept X

Se aplica a



Protección contra amenazas (Threat Protection) - Política Principal - Threat Protection:

New: Customers will get this feature gradually as computers update to the latest version of Sophos Intercept X

Protect network traffic

Detect malicious connections to command and control servers

Prevent malicious network traffic with packet inspection (IPS) New

New: Customers will get this feature gradually as computers update to the latest version of Core Agent

Detect malicious behavior New

New: Customers will get this feature gradually as computers update to the latest version of Core Agent

Adaptive active adversary protection

If disabled, active adversary behaviors are reported in Detections for XDR customers

AMSI Protection (with enhanced scan for script-based threats)

Prevent removal of AMSI registration

Advanced Settings

We recommend that you leave these set to the defaults. However, you might want to change them temporarily. Learn more

View advanced settings

Turn on anti-ransomware protection and all exploit mitigations ?

Turn on all exploit mitigation hooks

Scan trusted installers

Use recommended email attachment scanning

Deep learning detection level:

Default

Track network connections

Turn on event logging

Generate file hashes remotely for event logging

Periodically scan process memory in the background

SSL/TLS decryption of HTTPS websites

Decrypt HTTPS websites using SSL/TLS. If enabled it also turns on HTTPS decryption for Web Control

Note: You can exclude websites from decryption in the global settings pages

Device Isolation

Allow computers to isolate themselves on red health

Note: If a computer has red health, it will isolate itself from the network. It will still communicate with Sophos Central.

Scheduled Scanning

Scheduled Scanning

Enable scheduled scan

↑

↓

12 : 00 PM

↓

↑

SunMonTueWedThuFriSat

Enable deep scanning - scans inside archive files (.zip, .cab, etc.)

Exclusions

View Global Exclusions ?

Policy ExclusionsAdd Exclusion

EXCLUDE	ACTIVE FOR
There are currently no exclusions	

Desktop Messaging

Enable Desktop Messaging for Threat Protection

Configure a message to be added to the end of the standard notification

Por favor comunicarse con el departamento de sistemas.

Note: Custom messages will not be displayed for Intercept X events



Protección contra amenazas (Threat Protection) - Base Policy - Threat Protection:

New: Customers will get this feature gradually as computers update to the latest version of Sophos Intercept X

Protect network traffic

Detect malicious connections to command and control servers

Prevent malicious network traffic with packet inspection (IPS) New

New: Customers will get this feature gradually as computers update to the latest version of Core Agent

Detect malicious behavior New

New: Customers will get this feature gradually as computers update to the latest version of Core Agent

Adaptive active adversary protection

If disabled, active adversary behaviors are reported in Detections for XDR customers

AMSI Protection (with enhanced scan for script-based threats)

Prevent removal of AMSI registration

Advanced Settings

We recommend that you leave these set to the defaults. However, you might want to change them temporarily. [Learn more](#)

View advanced settings

Turn on anti-ransomware protection and all exploit mitigations ?

Turn on all exploit mitigation hooks

Scan trusted installers

Use recommended email attachment scanning

Deep learning detection level: Default

Track network connections

Turn on event logging

Generate file hashes remotely for event logging

Periodically scan process memory in the background

SSL/TLS decryption of HTTPS websites

Decrypt HTTPS websites using SSL/TLS. If enabled it also turns on HTTPS decryption for Web Control

Note: You can exclude websites from decryption in the [global settings pages](#)

Device Isolation

Allow computers to isolate themselves on red health

Note: If a computer has red health, it will isolate itself from the network. It will still communicate with Sophos Central.

Scheduled Scanning

Enable scheduled scan

1200PM

SunMonTueWedThuFriSat

Enable deep scanning - scans inside archive files (.zip, .cab, etc.)

Exclusions

View Global Exclusions ?

Policy Exclusions

Add Exclusion

EXCLUDE	ACTIVE FOR
There are currently no exclusions	

Desktop Messaging

Enable Desktop Messaging for Threat Protection

Configure a message to be added to the end of the standard notification

Por favor comunicarse con el departamento de sistemas.

Note: Custom messages will not be displayed for Intercept X events

✓✓

✓✓

✓

✓

✓

✓

Applies To
WindowsApple

✓✓

✓✓

✓✓

✓✓

✓✓

✓



Control de periféricos (Peripheral Control) - BIBLIOTECA:

Endpoint Protection - Ver política de ordenadores

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA*

BIBLIOTECA

GuardarCancelarEliminarClonar

TIPO DE POLÍTICA

Control de periféricos : Usuario

Última actualización22 nov. 2023

0 USUARIOS0 GRUPOSCONFIGURACIÓNPOLÍTICA OMITIDA

La política se omite: se ignora toda la configuración de esta política. La configuración procederá de otra política.

Administrar periféricos - configure las siguientes opciones de periféricos

☐

Desactivar el control de periféricos

☒

Supervisar pero no bloquear (se permitirán todos los periféricos)

☐

Controlar el acceso por tipo de periférico y añadir excepciones

Los totales que aparecen a continuación incluyen todos los periféricos detectados, ya sea en estaciones de trabajo o servidores:

Permitir

Bluetooth - 134 detectados

Permitir

Proteger almacenamiento extraíble - 0 detectados

Permitir

Disquete - 0 detectados

Permitir

Infrarrojo - 0 detectados

Permitir

Módem - 20 detectados

Permitir

Unidad óptica - 36 detectados

Permitir

Almacenamiento extraíble - 665 detectados

Permitir

Inalámbrico - 189 detectados

Permitir

MTP/PTP - 179 detectados

Excepciones de periféricos

Control de periféricos (Peripheral Control) - Política Principal - Peripheral Control:

Endpoint Protection - Ver política de ordenadores

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA*

Política Principal - Peripheral Control

GuardarCancelarEliminarClonar

TIPO DE POLÍTICA

Control de periféricos : Dispositivo

Última actualización18 oct. 2023

1 ORDENADORES0 GRUPOSCONFIGURACIÓNPOLÍTICA IMPUESTA

Administrar periféricos - configure las siguientes opciones de periféricos

☐

Desactivar el control de periféricos

☒

Supervisar pero no bloquear (se permitirán todos los periféricos)

☐

Controlar el acceso por tipo de periférico y añadir excepciones

Los totales que aparecen a continuación incluyen todos los periféricos detectados, ya sea en estaciones de trabajo o servidores:

Permitir

Bluetooth - 134 detectados

Permitir

Proteger almacenamiento extraíble - 0 detectados

Permitir

Disquete - 0 detectados

Permitir

Infrarrojo - 0 detectados

Permitir

Módem - 20 detectados

Permitir

Unidad óptica - 36 detectados

Permitir

Almacenamiento extraíble - 665 detectados

Permitir

Inalámbrico - 189 detectados

Permitir

MTP/PTP - 179 detectados

Excepciones de periféricos

Mensaje de escritorio

Control de periféricos (Peripheral Control) - Política base - Control de periféricos:

Endpoint Protection - Ver política de ordenadores

Alcaldía de Mosquera

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA: Política base - Control de periféricos

Guardar Cancelar Clonar Restablecer

TIPO DE POLÍTICA: Control de periféricos : Usuario

Última actualización: 18 oct. 2023

USUARIOS/ORDENADORES GRUPOS CONFIGURACIÓN POLÍTICA IMPUESTA

Administrar periféricos - configure las siguientes opciones de periféricos

☐ Desactivar el control de periféricos

☒ Supervisar pero no bloquear (se permitirán todos los periféricos)

☐ Controlar el acceso por tipo de periférico y añadir excepciones

Los totales que aparecen a continuación incluyen todos los periféricos detectados, ya sea en estaciones de trabajo o servidores:

Permitir	Bluetooth - 134 detectados
Permitir	Proteger almacenamiento extraíble - 0 detectados
Permitir	Disquete - 0 detectados
Permitir	Infrarrojo - 0 detectados
Permitir	Módem - 20 detectados
Permitir	Unidad óptica - 36 detectados
Permitir	Almacenamiento extraíble - 665 detectados
Permitir	Inalámbrico - 189 detectados
Permitir	MTP/PTP - 179 detectados

Excepciones de periféricos

Mensaje de escritorio



Control de Aplicaciones (Application Control) - Política Personalizada - Application Control:

Endpoint Protection - Ver política de ordenadores

Alcaldía de Mosquera

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA*

Política Personalizada - Application Control

GuardarCancelarEliminarClonar

TIPO DE POLÍTICA

Restricción de aplicaciones : Dispositivo

Última actualización20 oct. 2023

0 ORDENADORES0 GRUPOSCONFIGURACIÓNPOLÍTICA OMITIDA

La política se omite: se ignora toda la configuración de esta política. La configuración procederá de otra política.

Seleccione las aplicaciones que desea controlar y especifique las opciones de detección

Añadir/editar lista

Aplicaciones restringidas	Seleccionadas / total	Supervisar nuevas aplicaciones
> Vulnerabilidades de las aplicaciones	2 / 2	✓
> Herramienta de compresión	9 / 12	✓
> Herramienta de gestión de activos	20 / 21	✓
> Complemento del navegador	37 / 39	✓
> Herramienta de inteligencia comercial	49 / 49	✓
> Herramienta CRM	9 / 9	✓
> Herramienta de diseño	27 / 42	✓
> Buscador de escritorio	9 / 9	✓
> Procesado de imágenes	20 / 36	✓
> Computación distribuida	8 / 8	✓
> Visualizador de documentos	32 / 55	✓
> Gestor de descargas	63 / 65	✓
> Cliente de correo electrónico/PIM	26 / 34	✓
> Herramienta de sincronización de correo electrónico	3 / 4	✓
> Herramienta de cifrado/esteganografía	32 / 32	✓
> Software ERP	27 / 27	✓
> Aplicación de uso compartido de archivos	104 / 104	✓
> Cliente FTP	15 / 19	✓
> Juego	371 / 371	✓
> Mensajería instantánea	129 / 142	✓
> Navegador de Internet	102 / 122	✓
> Software de desbloqueo	3 / 3	✓
> Aplicación de mapas	3 / 6	
> Herramienta de conversión multimedia	3 / 19	
> Reproductor multimedia	122 / 145	✓
> Sincronización móvil	35 / 41	✓
> Herramienta de motorización de red / vulnerabilidades	66 / 66	✓
> Suite de ofimática	31 / 49	✓

NIT: 901161495-0
BOGOTÁ AV. CARRERA 15 #119-11. OFICINA 502

Control de Aplicaciones (Application Control) - Política Personalizada -
Application Control:

>	Almacenamiento en línea	80 / 91	✓
>	Herramienta para grabar discos ópticos	20 / 22	✓
>	Emulación de unidad óptica	2 / 5	✓
>	Herramienta de recuperación de contraseñas / licencias	32 / 32	✓
>	Software de bromas	2 / 2	✓
>	Herramienta de privacidad	15 / 15	✓
>	Herramienta de programación/descriptivo	54 / 66	✓
>	Herramienta proxy/VPN	133 / 137	✓
>	Herramienta de administración remota	123 / 128	✓
>	Entorno en tiempo de ejecución	5 / 7	✓
>	Herramienta de captura de pantalla	25 / 25	✓
>	Aplicación de protector de pantalla	11 / 11	✓
>	Herramienta de seguridad	88 / 89	✓
>	Actualizador de software	18 / 33	✓
>	Herramienta del sistema	228 / 261	✓
>	Cliente Telnet	3 / 7	✓
>	Herramienta de conexión mediante catering	15 / 15	✓

>	Barra de herramientas	83 / 83	✓
>	Lanzadera de programas USB	9 / 9	✓
>	Aplicación de virtualización	30 / 30	✓
>	Voz sobre IP	38 / 46	✓

Opciones de detección

☒ Detectar aplicaciones restringidas cuando los usuarios accedan (recibirá una notificación)

☐ Permitir la aplicación detectada

☒ Bloquear la aplicación detectada

☒ Detectar aplicaciones restringidas durante los escaneos programados y en demanda

Puede solicitar que Sophos añada aplicaciones

[Solicitud de restricción de aplicaciones](#)

Mensaje de escritorio

☒ Activar los mensajes de escritorio para el control de aplicaciones

Configurar un mensaje para añadirlo al final de la notificación estándar

Nota: Los mensajes personalizados no se mostrarán para eventos Intercept X.



Control de Aplicaciones (Application Control) - Política Principal - Application Control:

Endpoint Protection - Ver política de ordenadores

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA*

Política Principal - Application Control

GuardarCancelarEliminarClonar

TIPO DE POLÍTICA

Restricción de aplicaciones : Dispositivo

Última actualización18 oct. 2023

1 ORDENADORES0 GRUPOSCONFIGURACIÓNPOLÍTICA IMPUESTA

Seleccione las aplicaciones que desea controlar y especifique las opciones de detección

Añadir/editar lista

Aplicaciones restringidas	Seleccionadas / total	Supervisar nuevas aplicaciones
> Vulnerabilidades de las aplicaciones	2 / 2	✓
> Complemento del navegador	37 / 39	✓
> Juego	371 / 371	✓
> Herramienta proxy/VPN	133 / 137	✓
> Barra de herramientas	83 / 83	✓

Opciones de detección

☒ Detectar aplicaciones restringidas cuando los usuarios accedan (recibirá una notificación)

☐ Permitir la aplicación detectada

☒ Bloquear la aplicación detectada

☒ Detectar aplicaciones restringidas durante los escaneos programados y en demanda

Puede solicitar que Sophos añada aplicaciones

Solicitud de restricción de aplicaciones

Control de Aplicaciones (Application Control) - Política base - Restricción de aplicaciones:

Endpoint Protection - Ver política de ordenadores

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA

Política base - Restricción de aplicaciones

GuardarCancelarClonarRestablecer

TIPO DE POLÍTICA

Restricción de aplicaciones : Usuario

Última actualización24 oct. 2023

USUARIOS/ORDENADORESGRUPOSCONFIGURACIÓNPOLÍTICA IMPUESTA

Seleccione las aplicaciones que desea controlar y especifique las opciones de detección

Añadir/editar lista

Aplicaciones restringidas	Seleccionadas / total	Supervisar nuevas aplicaciones
> Vulnerabilidades de las aplicaciones	2 / 2	✓
> Complemento del navegador	37 / 39	✓
> Juego	370 / 371	✓
> Herramienta proxy/VPN	133 / 137	✓
> Barra de herramientas	83 / 83	✓

Opciones de detección

☒ Detectar aplicaciones restringidas cuando los usuarios accedan (recibirá una notificación)

☐ Permitir la aplicación detectada

☒ Bloquear la aplicación detectada

☒ Detectar aplicaciones restringidas durante los escaneos programados y en demanda

Puede solicitar que Sophos añada aplicaciones

Solicitud de restricción de aplicaciones



Prevencción de pérdida de datos (Data Loss Prevention) - Política Principal - Data Loss Prevention:

Introducción / Políticas de ordenador / Ver política de ordenador

Alcaldía de Mosquera

NOMBRE DE POLÍTICA*

Política Principal - Data Loss Prevention

GuardarCancelarEliminarClonar

TIPO DE POLÍTICA

Prevencción de pérdida de datos : Dispositivo

1 ORDENADORES0 GRUPOS

CONFIGURACIÓN

POLÍTICA IMPUESTA

Usar reglas para transferencias de datos

Configuración de reglas de archivo

NOMBRE	DLP MONITOR
DESCRIPCIÓN	DLP MONITOR
CONDICIONES	<div>Tiños de archivo:</div> <div><div>Documento</div><div>Base de datos</div><div>Hoja de cálculo</div><div>Presentación</div></div> <div>El destino es:</div> <div><div>Programa de correo electrónico</div><div>Navegador de Internet</div><div>Mensajería instantánea</div><div>Navegador de Internet - procesos externos</div><div>Voz sobre IP</div><div>Almacenamiento</div></div>
EXCLUSIONES	
ACCIÓN	Permitir transferencia

Prevencción de pérdida de datos (Data Loss Prevention) - Política base - Prevencción de pérdida de datos:

Introducción / Políticas de ordenador / Ver política de ordenador

Alcaldía de Mosquera

NOMBRE DE POLÍTICA

Política base - Prevencción de pérdida de datos

GuardarCancelarClonarRestablecer

TIPO DE POLÍTICA

Prevencción de pérdida de datos : Usuario

USUARIOS/ORDENADORESGRUPOS

CONFIGURACIÓN

POLÍTICA IMPUESTA

Usar reglas para transferencias de datos

Configuración de reglas de archivo

NOMBRE	DLP MONITO
DESCRIPCIÓN	DLP MONITOR
CONDICIONES	<div>Tiños de archivo:</div> <div><div>Documento</div><div>Base de datos</div><div>Hoja de cálculo</div><div>Presentación</div></div> <div>El destino es:</div> <div><div>Programa de correo electrónico</div><div>Navegador de Internet</div><div>Mensajería instantánea</div><div>Navegador de Internet - procesos externos</div><div>Voz sobre IP</div><div>Almacenamiento</div></div>
EXCLUSIONES	
ACCIÓN	Permitir transferencia



Control Web (Web Control) - CAD:

Endpoint Protection - Ver política de ordenadores

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA*

CAD

GuardarCancelarEliminarClonar

TIPO DE POLÍTICA

Control web

Última actualización22 nov. 2023

0 USUARIOS1 GRUPOS CONFIGURACIÓN POLÍTICA IMPUESTA

Control web

Imponer las opciones en esta sección de la política

Nota: Si el descifrado HTTPS está activado en la política de protección contra amenazas para un dispositivo, también se utilizará para las comprobaciones de la política de control web en el mismo dispositivo. Puede excluir sitios del descifrado en la página Configuración.

Opciones de seguridad adicionales

Bloquear descargas peligrosasVer detalles

Uso web aceptable

Mantener limpioVer detalles

Proteger contra la pérdida de datos

Permitir uso compartido de datosVer detalles

Registrar eventos de control web - Se registrarán y serán visibles en los informes todos los intentos de visitar sitios bloqueados, junto con los avisos y los casos en los que se ignoren dichos avisos.

Controlar sitios etiquetados en la Administración de sitios web

Etiquetas de sitios web

BLOQUEAR

Acciones

Bloquear

Añadir nuevo

Aplicar esta política de control web solo a periodos definidos

Control Web (Web Control) - Política Principal - Web Control:

Endpoint Protection - Ver política de ordenadores

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA*

Política Principal - Web Control

GuardarCancelarEliminarClonar

TIPO DE POLÍTICA

Control web

Última actualización20 oct. 2023

4 USUARIOS0 GRUPOS CONFIGURACIÓN POLÍTICA OMITIDA

La política se omite: se ignora toda la configuración de esta política. La configuración procederá de otra política.

Control web

Imponer las opciones en esta sección de la política

Nota: Si el descifrado HTTPS está activado en la política de protección contra amenazas para un dispositivo, también se utilizará para las comprobaciones de la política de control web en el mismo dispositivo. Puede excluir sitios del descifrado en la página Configuración.

Opciones de seguridad adicionales

Bloquear descargas peligrosasVer detalles

Uso web aceptable

Mantener limpioVer detalles

Proteger contra la pérdida de datos

Permitir uso compartido de datosVer detalles

Registrar eventos de control web - Se registrarán y serán visibles en los informes todos los intentos de visitar sitios bloqueados, junto con los avisos y los casos en los que se ignoren dichos avisos.

Controlar sitios etiquetados en la Administración de sitios web

Etiquetas de sitios web

No ha añadido ningún filtro web personalizado.
Haga clic en el botón Añadir nuevo para añadir un filtro web.

Acciones

Añadir nuevo

Aplicar esta política de control web solo a periodos definidos

NIT: 901161495-0

BOGOTÁ AV. CARRERA 15 #119-11. OFICINA 502

Control Web (Web Control) - Política base - Control web:

Endpoint Protection - Ver política de ordenadores

Alcaldía de Mosquera

Introducción / Políticas de ordenador / Ver política de ordenador

NOMBRE DE POLÍTICA

Política base - Control web

Guardar

Cancelar

Clonar

Restablecer

TIPO DE POLÍTICA

Control web

Última actualización

27 oct. 2023

USUARIOS/ORDENADORES

GRUPOS

CONFIGURACIÓN

POLÍTICA IMPUESTA

Control web

Imponer las opciones en esta sección de la política

Nota: Si el descifrado HTTPS está activado en la política de protección contra amenazas para un dispositivo, también se utilizará para las comprobaciones de la política de control web en el mismo dispositivo. Puede excluir sitios del descifrado en la página Configuración.

Opciones de seguridad adicionales

Bloquear descargas peligrosas

Ver detalles

Uso web aceptable

Mantener limpio

Ver detalles

Proteger contra la pérdida de datos

Permitir uso compartido de datos

Ver detalles

Registrar eventos de control web

Se registrarán y serán visibles en los informes todos los intentos de visitar sitios bloqueados, junto con los avisos y los casos en los que se ignoren dichos avisos.

Controlar sitios etiquetados en la Administración de sitios web

Añadir nuevo

Etiquetas de sitios web	Acciones
Traductores	Permitir



Dispositivos

Equipos:

Estaciones de Trabajo Administradas: 357 Dispositivos registrados.
Dispositivos con Alertas Amarillas y Rojas: 24 Dispositivos.

Endpoint Protection - Ordenadores

Introducción / Panel de control de Endpoint Protection / Ordenadores

Ordenadores

Ordenadores no administrados

Grupos de equipos

Gestionar software de estaciones

Activar la protección contra manipulaciones

Restablecer el estado de seguridad

Eliminar

Exportar a un archivo de valores separados por coma (CSV)

Todos los ordenadores

Mostrar todos los equipos

Cualquier tipo de protección

Todos

Q Buscar

☐	Nombre	IP	SO	Protección	Último usuario	Última vez activo	Grupo	Protección contra manipulaciones
☐	CUL1009184	192.168.105.105	Windows 11 Pro	✓ Intercept X Advanced with XDR	Javier.Trujillo	23 de nov. de 2023 15:11		Activado
☐	GRC999393	192.168.14.178	Windows 10 Pro	✓ Intercept X Advanced with XDR	Mariann.Bonilla	23 de nov. de 2023 15:11		Activado
☐	SAL29623	192.168.10.219	Windows 10 Pro	✓ Intercept X Advanced with XDR	Yazmin.Penagos	23 de nov. de 2023 15:11		Activado
☐	PLAN1002035	192.168.13.189	Windows 10 Pro	✓ Intercept X Advanced with XDR	Nelly.Quintana	23 de nov. de 2023 15:10		Activado
☐	DSO1007869	192.168.10.231	Windows 10 Pro	✓ Intercept X Advanced with XDR	Lina.Rodriguez	23 de nov. de 2023 15:09		Activado
☐	IMac de PRENSAMC2	192.168.14.105	macOS Monterey 12.5	✓ Intercept X Advanced with XDR	usuarioprensa	23 de nov. de 2023 15:09		Activado
☐	JUR1002014	192.168.12.107	Windows 11 Pro	✓ Intercept X Advanced with XDR	Zully.Jimenez	23 de nov. de 2023 15:09		Activado
☐	PROS49057	192.168.115.239	Windows 10 Pro for Workstations	✓ Intercept X Advanced with XDR	John.Caro	23 de nov. de 2023 15:09		Activado
☐	SMF1008159	192.168.108.39	Windows 11 Pro	✓ Intercept X Advanced with XDR	Liz.Diaz	23 de nov. de 2023 15:09		Activado
☐	CUL48852	192.168.105.200	Windows 10 Pro	✓ Intercept X Advanced with XDR	Sonia.Jimenez	23 de nov. de 2023 15:08		Activado
☐	GRC48808	192.168.14.234	Windows 10 Pro	✓ Intercept X Advanced with XDR	Diana.Mendoza	23 de nov. de 2023 15:08		Activado
☐	COM1000409	192.168.14.238	Windows 10 Pro	✓ Intercept X Advanced with XDR	Jennifer.Rojas	23 de nov. de 2023 15:07		Activado
☐	ISP1001170	192.168.12.113	Windows 10 Pro	✓ Intercept X Advanced with XDR	Lizet.Alarcon	23 de nov. de 2023 15:06		Activado

1 - 250 de 357 ordenadores / 0 seleccionados

<<

<

1

2

>

>>

Última actualización: 23 nov. 2023, 15:11



Exclusiones globales (Global Exclusions)

Exclusiones Recomendadas por Sophos y Microsoft

Configuración global / Exclusiones globales		Alcalde de Mosquera	
%allusersprofile%\NTUser.pol Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%SystemRoot%\System32\GroupPolicy\Machine\Registry.pol Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%SystemRoot%\System32\GroupPolicy\Machine\Registry.tmp Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%SystemRoot%\System32\GroupPolicy\User\Registry.pol Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%SystemRoot%\System32\GroupPolicy\User\Registry.tmp Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%temp%**DOCU.exe Archivo o carpeta (Windows)	En tiempo real y programado	Software "DOCU" Secretaría Planeación , Con exclusión de Microsoft Access	⌕
%userprofile%\NTUser.dat* Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%windir%\Security\Database*.chk Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%windir%\Security\Database*.cmx Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%windir%\Security\Database*.csv Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%windir%\Security\Database*.edb Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%windir%\Security\Database*.jrs Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%windir%\Security\Database*.log Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%windir%\Security\Database*.sdb Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%windir%\Security\Database*.xml Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%windir%\SoftwareDistribution\Datastore\Datastore.edb Archivo o carpeta (Windows)	En tiempo real y programado	Recommended vendor exclusions for use with Sophos products on Windows	⌕
%windir%\SoftwareDistribution\Datastore\Logs\Edb*.jrs	En tiempo real y	Recommended vendor exclusions for use with	⌕



Roles de administración

Los roles de administración dividen la administración de seguridad en función del nivel de responsabilidad. Sophos Central incluye varios roles predefinidos.

El rol de administrador que tiene asignado determina lo que puede hacer.

Administración de roles

Alcaldía de Mosquera

Configuración global / Administración de roles

Buscar

Añadir rol

Eliminar

Nombre	# administradores	Tipo	Descripción
Superadministrador	2	Predefinido	El rol de superadministrador es un rol predefinido que tiene acceso a todo en Sophos Central.
Administrador	0	Predefinido	El rol de administrador es un rol predefinido que tiene acceso a casi todo como el superadministrador, excepto la capacidad para administrar roles y asignaciones de roles.
Soporte técnico	0	Predefinido	El rol de servicio de asistencia es un rol predefinido que permite al administrador tomar ciertas medidas administrativas. Más información
Solo lectura	0	Predefinido	El rol de solo lectura es un rol predefinido que tiene acceso de solo lectura a todo en Sophos Central.

Superadministrador

Alcaldía de Mosquera

Configuración global / Administración de roles / SuperAdmin

★

Superadministrador

Nota: Este es un rol proporcionado por el sistema. No puede eliminar ni editar este rol

Descripción

El rol de superadministrador es un rol predefinido que tiene acceso a todo en Sophos Central.

Permisos

	Completa	Soporte técnico	Solo lectura
Sophos Central Admin	✓		

Configuración global para Sophos Central Admin

Función	Activado
Acceder a registros e informes confidenciales	✓
Acceder a administración de políticas	✓
Acceder a asignación de políticas	✓
Activar la gestión de la búsqueda global	✓

Miembros de rol (2)

Editar

Alcaldía Mosquera

Dirección TIC

APROBACIÓN DE CONFIGURACIÓN

Por medio de la presente se deja constancia la aceptación de la configuración realizada a la solución Sophos Central, según lo establecido en el alcance y las pruebas realizadas en conjunto con el equipo de Alcaldía de Mosquera, siendo estas todas satisfactorias.

Se entrega informe de configuración de la Implementación de Sophos Central, realizado por la Gerencia de ingeniería e implementación de Corporación Maestre.

En Bogotá, a los Veinticuatro (24) días del mes de Noviembre de 2023

Yessika Salazar
Gerente. de Ingeniería e Implementación
CORPORACIÓN MAESTRE, S.A.S

Jeofrey Sulbaran
Ing. Implementación y Soporte
CORPORACIÓN MAESTRE, S.A.S

Conforme Aprueba
Mireya Calderon
Supervisora del Contrato
ALCALDÍA DE MOSQUERA