Guía de Seguridad de las TIC
CCN-STIC 1222

Procedimiento de Empleo Seguro
Cortex XDR Agent

Julio 2026

Edita:

centro criptológico nacional

Centro Criptológico Nacional, 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.07.28 08:19:50 +02'00'

ÍNDICE

1 INTRODUCCIÓN

1. La plataforma Cortex XDR de Palo Alto Networks ofrece seguridad para el endpoint de última generación, deteniendo las amenazas más sofisticadas mediante un enfoque multicapa. Combina la prevención basada en Inteligencia Artificial (IA) y Aprendizaje Automático (ML) con una protección avanzada contra exploits y amenazas de comportamiento. Toda esta capacidad se integra en una plataforma unificada que correlaciona datos de telemetría del endpoint, la red, la nube y la identidad para proporcionar una detección y respuesta extendidas (XDR).
2. Cortex XDR está diseñado para romper los silos de seguridad tradicionales. El despliegue de su agente ligero y único no solo reemplaza a los antivirus heredados, sino que establece la base para una estrategia de seguridad evolutiva. A medida que una organización madura, puede expandir sus capacidades hacia una cobertura XDR completa o incluso evolucionar hacia una plataforma de operaciones de seguridad (SOC) autónoma con Cortex XSIAM (u otro), todo ello sin necesidad de redesplegar o añadir agentes en los endpoints.
3. Las capacidades de protección del agente Cortex XDR son exhaustivas y operan de forma autónoma, garantizando la seguridad del equipo tanto si está conectado a la red como si no. Dispone de múltiples motores de protección especializados: un motor de análisis local basado en IA para identificar malware conocido y desconocido, un motor anti-exploit para bloquear las técnicas de explotación de vulnerabilidades, y un motor de protección contra amenazas de comportamiento que detecta las Tácticas, Técnicas y Procedimientos (TTPs) de los atacantes. Este enfoque multicapa maximiza la eficacia en la detección, minimiza los falsos positivos y optimiza el consumo de recursos del sistema.
4. Cortex XDR ofrece la solución ideal para consolidar la seguridad del endpoint, combinando la prevención más eficaz con una visibilidad completa de la cadena de ataque, simplificando la arquitectura de seguridad a través de una única plataforma y agente.
5. Proporciona protección frente a un amplio espectro de ataques, desde malware común hasta las amenazas más evasivas y ataques sin ficheros (*fileless*), utilizando los siguientes mecanismos de protección y prevención:
    a) **Análisis Local con Inteligencia Artificial**: Un motor de ML integrado en el agente que analiza estáticamente los ficheros para detectar y bloquear malware conocido y de día cero (*zero-day*), incluyendo todo tipo de ransomware, antes de su ejecución.
    b) **Protección Anti-Exploit**: Previene y bloquea las técnicas utilizadas por los atacantes para explotar vulnerabilidades de software en el sistema operativo o en las aplicaciones, deteniendo la amenaza en las fases iniciales del ataque.
    c) **Protección contra Amenazas de Comportamiento (BIOC)**: Identifica y detiene ataques sofisticados, incluyendo los que no utilizan ficheros, mediante el análisis continuo del comportamiento de los procesos y la detección de Indicadores de Compromiso por comportamiento (BIOCs).
    d) **Reglas de Detección Personalizables (IOC y BIOC)**: Permite a los equipos de seguridad crear sus propias reglas de detección y buscar Indicadores de Compromiso (IOCs) y de Comportamiento (BIOCs) en toda la organización.

e) **Capacidad de Respuesta en el Endpoint**: Permite aislar un equipo de la red, poner ficheros en cuarentena para su análisis y finalizar procesos maliciosos directamente desde la consola.

f) **Control de Scripts**: Ofrece visibilidad y control granular sobre la ejecución de scripts, como PowerShell, VBScript y macros de Office, para bloquear su uso malicioso.

g) **Protección del Agente (Anti-Tampering)**: Impide la desinstalación, detención o manipulación no autorizada del agente, incluso por parte de usuarios con privilegios de administrador local.

6. Adicionalmente, Cortex XDR agiliza las operaciones de seguridad y la respuesta a incidentes:

a) **Análisis de Causa Raíz**: Elimina las conjeturas al revelar automáticamente la secuencia completa y el origen de cada alerta.

b) **Visualización de la Cadena de Causalidad**: Presenta los ataques en un árbol de procesos fácil de interpretar, enriquecido con todo el contexto necesario para entender el alcance del incidente.

c) **Mapeo Automático con MITRE ATT&CK®**: Clasifica las alertas según las tácticas y técnicas del framework de MITRE, facilitando la comprensión inmediata de las acciones del adversario y acelerando la investigación.

d) **Aplicación de playbooks de automatización:** Cortex XDR integra capacidades de automatización mediante playbooks, que son flujos de trabajo que estandarizan y aceleran la respuesta a incidentes. Un playbook ejecuta una secuencia de tareas, como scripts para enriquecer alertas o acciones de remediación, orquestando la investigación. Los analistas pueden utilizar una librería de playbooks predefinidos o crear los suyos para automatizar tareas repetitivas de forma consistente.

2 OBJETO Y ALCANCE

7. En este documento se indican los pasos a seguir para conseguir que las funciones de Cortex XDR comentadas en el apartado anterior sean operativas, atendiendo a unos requisitos de seguridad que aseguren el uso del producto de forma correcta y segura.

8. Para aplicar la configuración, en esta guía se detalla el proceso de instalación, indicando los diferentes requisitos que se deben cumplir, y con la ayuda de imágenes que facilitan al lector el proceso.

9. Adicionalmente se incluye la preparación del entorno operacional atendiendo a las distintas necesidades que definen las características operativas y lógicas del producto.

10. El presente documento incluye los enlaces de descarga de los programas necesarios, como los agentes que deben ser descargados para luego introducirse en los endpoints, y los servicios que son usados por el producto, como la interfaz web Cortex XDR, así como la utilización de estos.

11. Cortex XDR Agent es un producto software cuya instalación se realiza en los endpoints, y se gestiona desde una consola en la nube.

12. **El agente de Cortex XDR, versión 9.0, sobre el Sistema Operativo Windows, que se incluye tanto en Cortex XDR Prevent (EPP) como en Cortex XDR Pro (EPP, EDR, NTA, UEBA),** ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF20]**.**

13. Las versiones del Sistema Operativo Windows soportadas por Cortex XDR vienen indicadas en Where Can I Install the Cortex XDR Agent? [REF19], en la web de documentación de Palo Alto Networks (docs-cortex.paloaltonetworks.com/p/XDR [REF1]).

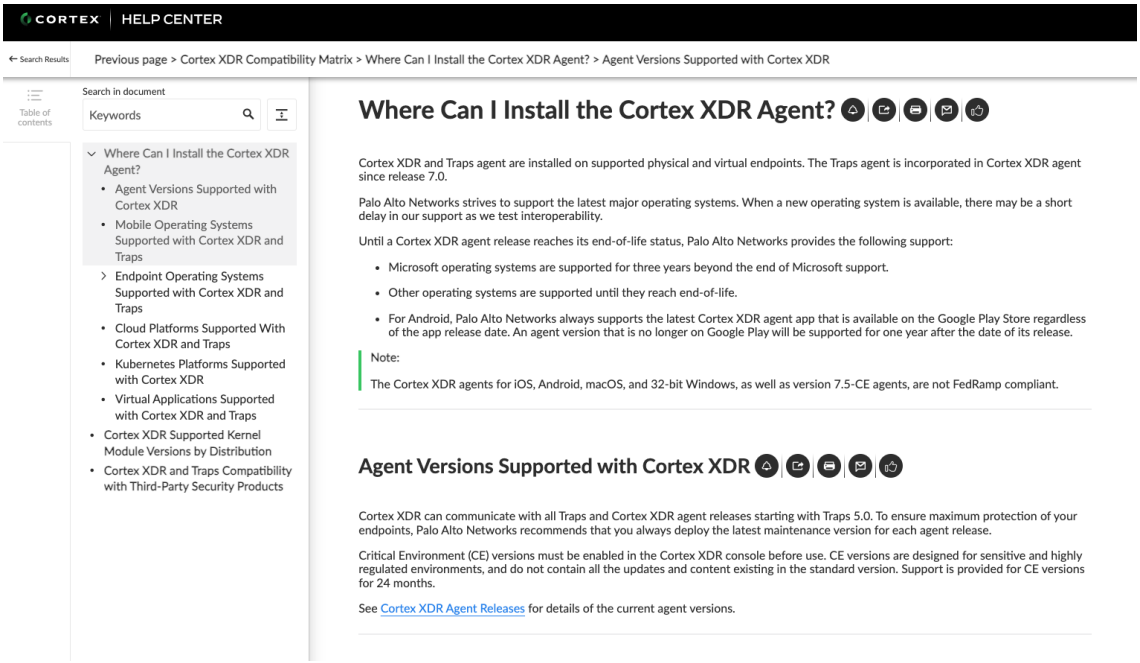

Ilustración 1. Referencia de Sistemas Operativos Soportados

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración y operación del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

14. La organización recibirá por parte de Palo Alto Networks un enlace de activación del *tenant*, así como instrucciones para la activación de este, y el acceso al portal de soporte de cliente (CSP, *Customer Support Portal* [REF2]).

15. Únicamente un usuario verificado por Palo Alto Networks podrá activar el *tenant*, tras establecer su MFA (*Multi-Factor Authentication*). En caso de tratarse de un cliente nuevo, deberá hacer uso de su cuenta de usuario del portal de soporte (CSP). En caso de tratarse de un usuario ya existente, deberá hacer uso de un perfil de usuario con permisos de Super User, asociado a la cuenta de la organización.

16. El agente sólo podrá ser generado y descargado una vez activado el *tenant* por parte del usuario. Solo deben utilizarse agentes descargados del *tenant* de la organización. Cualquier modificación sobre el mismo impedirá su conexión y uso, garantizando la entrega segura del mismo.

17. Puede verificarse la integridad del agente descargado comprobando que está firmado con el certificado: *0e 59 b3 82 cd a8 d1 9b da f0 e4 22 42 63 39 c1* de *Palo Alto Networks (Netherlands) B.V.*

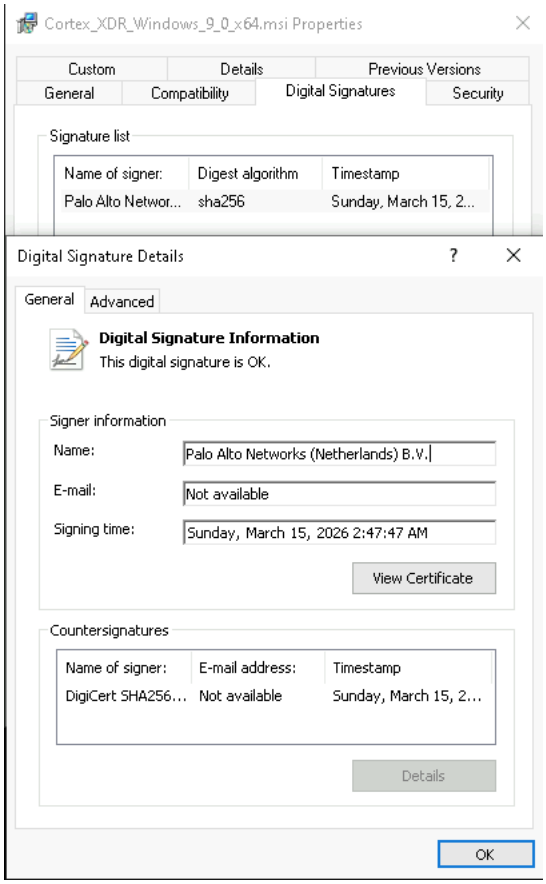

Ilustración 2. Certificado de Palo Alto Networks (Netherlands) B. V.

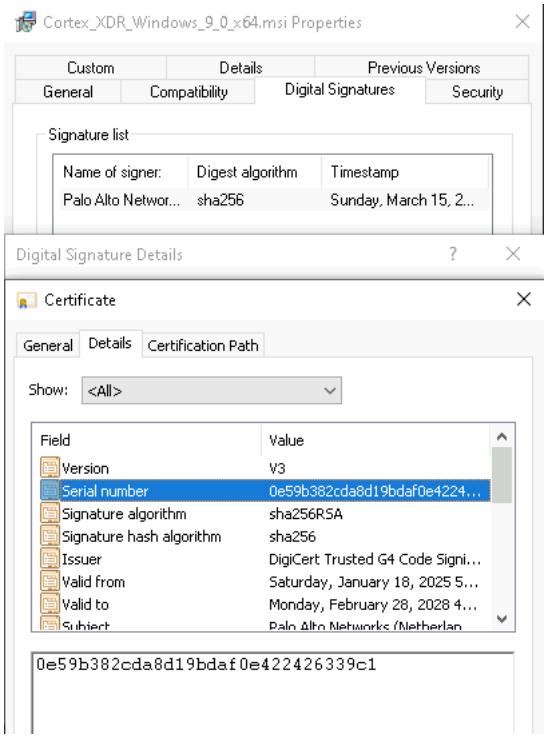

Ilustración 3. Número de serie del Certificado de Palo Alto Networks

4.2 ENTORNO DE INSTALACIÓN SEGURO

18. Al ser una plataforma SaaS, se provisionan recursos y se generan los accesos a la plataforma donde opera el servicio.
19. El instalador del agente debe ser descargado directamente desde la consola de Cortex XDR de la organización. Esto asegura que el paquete es auténtico, no ha sido manipulado y contiene la configuración de seguridad y la clave de comunicación correctas para el tenant de la organización.
20. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para las comunicaciones seguras. Para conocer los dominios a habilitar para las comunicaciones con la nube de Palo Alto Networks visitar el apartado del documento "6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS".

4.3 REGISTRO Y LICENCIAS

21. La referencia para el proceso de registro del tenant se encuentra en Activate Cortex XDR [REF3], en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com [REF1]).
22. Desde el cuadro de diálogo **Settings > Cortex XDR License** (Licencia de Cortex XDR), se puede ver el tipo de licencia asociado con su instancia de Cortex XDR.
23. Para cada licencia, Cortex XDR muestra un mosaico que contiene la fecha de vencimiento de la licencia, y detalles adicionales específicos del tipo de licencia:

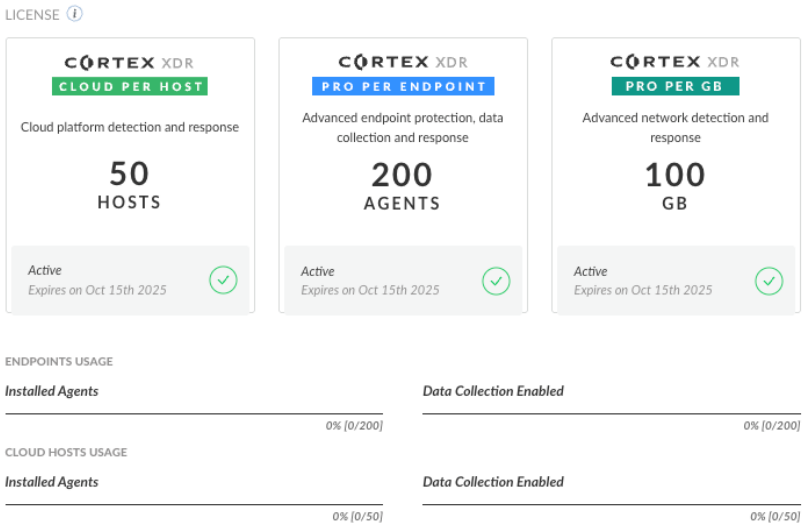

Ilustración 4. Detalle de licencias

Licencia	Detalles del mosaico
Cortex XDR Prevent	Muestra el número total de agentes concurrentes permitidos por la licencia. También es posible ver un gráfico de la asignación de licencia actual (total y porcentaje).
Cortex XDR Pro per endpoint	Muestra el número total de agentes instalados, además del número y porcentaje de agentes con funciones Pro habilitadas. Debajo del mosaico de licencia, también se puede ver la política de retención de almacenamiento, la cantidad total de almacenamiento asignada para la recopilación de datos mejorada y el uso real de datos.
Cortex XDR Pro per GB	Muestra la cantidad de almacenamiento total incluida con su licencia y la fecha de caducidad de la licencia. El almacenamiento usado se ve desde
Combinación de Cortex XDR Pro per endpoint y Cortex XDR Pro per GB	Cortex XDR Pro per Endpoint muestra el número total de agentes instalados, mientras que Cortex XDR Pro per GB muestra cuántos agentes están habilitados con la recopilación de datos de endpoint, lo que les permite recopilar y enviar datos al servidor.
Complementos	
Host Insights	Muestra el número de licencias adquiridas y el número y porcentaje usadas. También se puede ver vencimiento de la licencia.
Forensics	Muestra el número de licencias adquiridas y el número y porcentaje usadas. También se puede ver vencimiento de la licencia.
Identity Threat	Muestra el número de licencias adquiridas. También se puede ver vencimiento de la licencia.
Compute Units	Muestra el número de unidades de cómputo adquiridas. También se puede ver vencimiento de la licencia.
Extended Threat Hunting Data	Muestra el número de licencias adquiridas y el número y porcentaje usadas. También se puede ver vencimiento de la licencia.

Tabla 1. Detalle específico del tipo de licenciamiento y complementos

4.4 CONSIDERACIONES PREVIAS

24. La conexión saliente del agente se realiza mediante conexión SSL por el puerto 443. Si se usa descifrado SSL pueden experimentarse dificultades con la conexión de los agentes con la consola.
25. El agente se generará y descargará siguiendo el manual del producto.
26. El proceso de creación de un paquete de instalación de Agente se puede consultar en el enlace Create an Agent Installation Package [REF4], en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com [REF1].

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

27. El único componente del entorno de operación es el propio servidor Cortex XDR al que se conectará el agente.

5 FASE DE INSTALACIÓN

28. El agente se instalará siguiendo la guía Install the Cortex® XDR™ Agent for Windows en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com [REF1]).
29. Las versiones del Sistema Operativo Windows soportadas por Cortex XDR vienen indicadas en Where Can I Install the Cortex XDR Agent? [REF19], en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com [REF1]).

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

6.1.1 CONFIGURACIÓN DE AGENTES

6.1.1.1 CREACIÓN DE PERFIL

30. Para llevar a cabo la configuración de los agentes, es necesario acceder a la URI que fue generada para la gestión del sistema, durante la activación de la consola en la nube siguiendo el proceso indicado en la guía Activate [REF3] en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com [REF1]).
31. En dicha URI, es necesario que se proceda a habilitar la funcionalidad de EDR.
32. Para ello, hay que navegar dentro del site al menú de "**Endpoints**", y seleccionar "**Policy Management**".

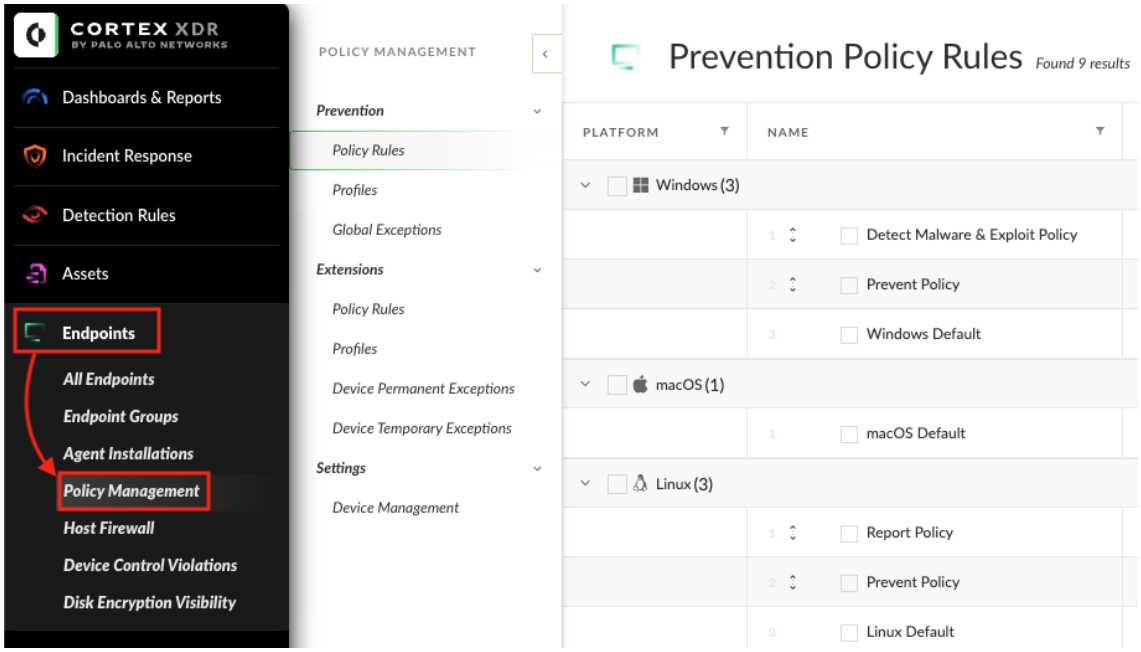

Ilustración 5. Policy Management

33. En el menú que se mostrará, es necesario entonces navegar en el menú "**PREVENTION**" a la opción "**Profiles**".

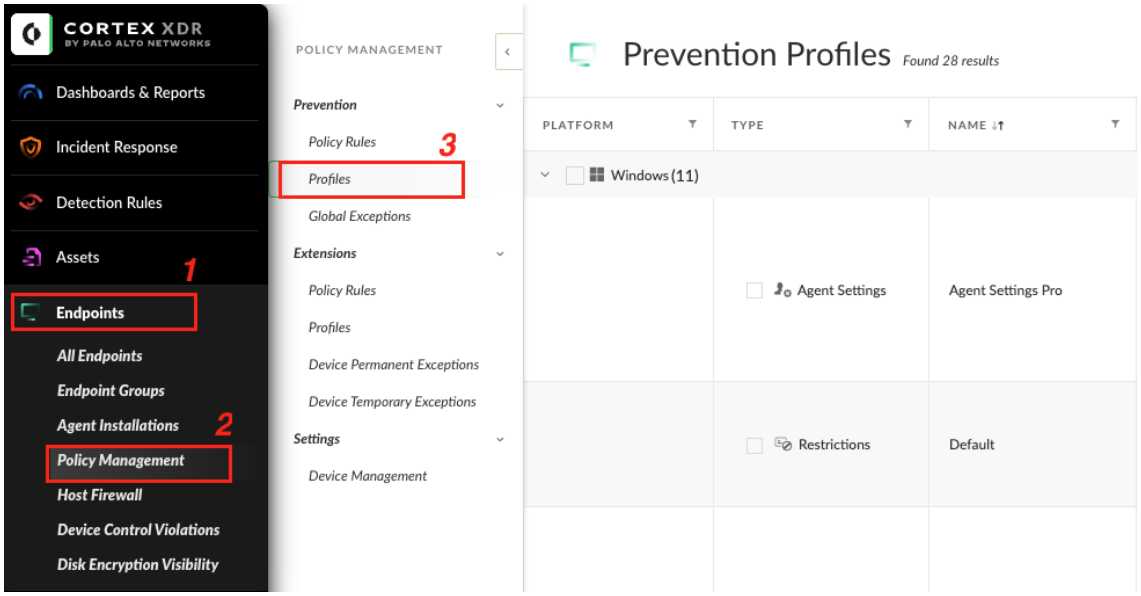

Ilustración 6. Prevention Policy Rules

34. En este menú, existe ya la posibilidad de crear un nuevo perfil de políticas, haciendo clic en el botón "**+ New Profile**".

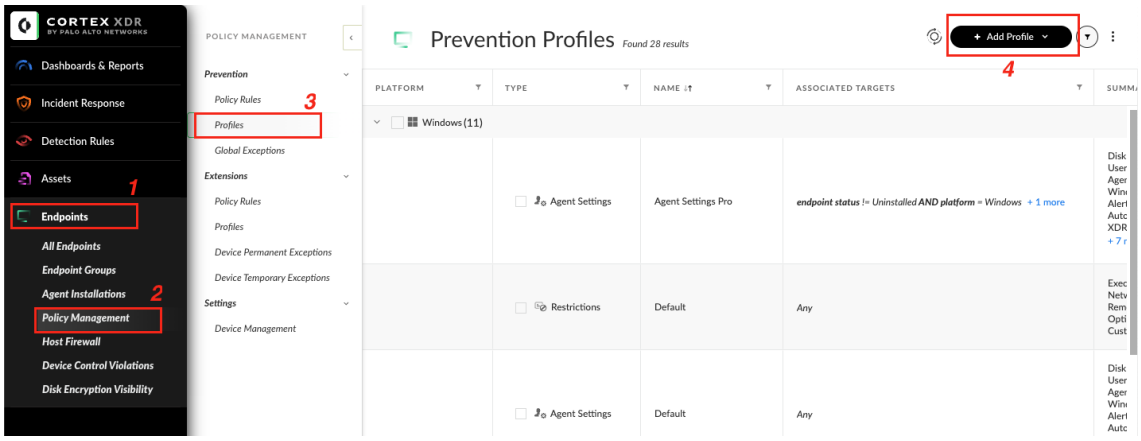

Ilustración 7. Prevention Profiles

35. En la nueva pantalla, se deberá escoger el Sistema Operativo de los agentes a ser usados por el usuario final.

> ***NOTA**: Se deberá de crear un perfil por cada uno de los Sistemas Operativos de destino donde estará operativa la solución. Por ejemplo, si se hace uso de los agentes de Windows y Mac, estos pasos se deberán ejecutar 2 veces.*

36. Una vez seleccionado el Sistema Operativo, se deberá de seleccionar la opción "**Agent Settings**", y hacer clic en "**Next**". En la siguiente imagen se ilustran los pasos para el Sistema Operativo Windows:

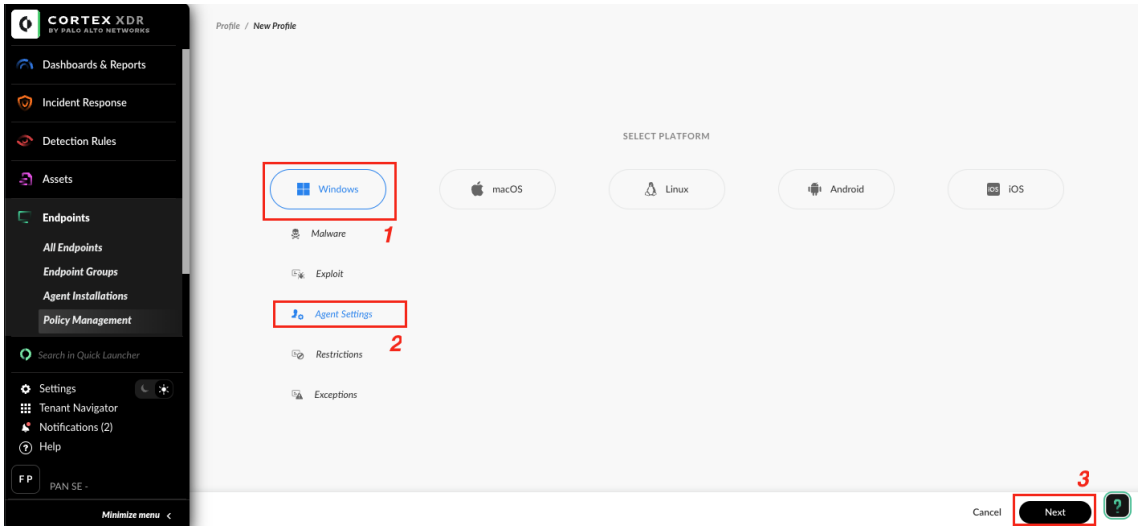

Ilustración 8. Agent Settings

37. En el nuevo menú que se despliega sobre las opciones del agente, es necesario navegar a "**Monitor and Collect Enhanced Endpoint Data**", y cambiar la opción por defecto, ya que se encuentra deshabilitada, y seleccionar bajo "**ACTION MODE**" la opción "**Enabled**".

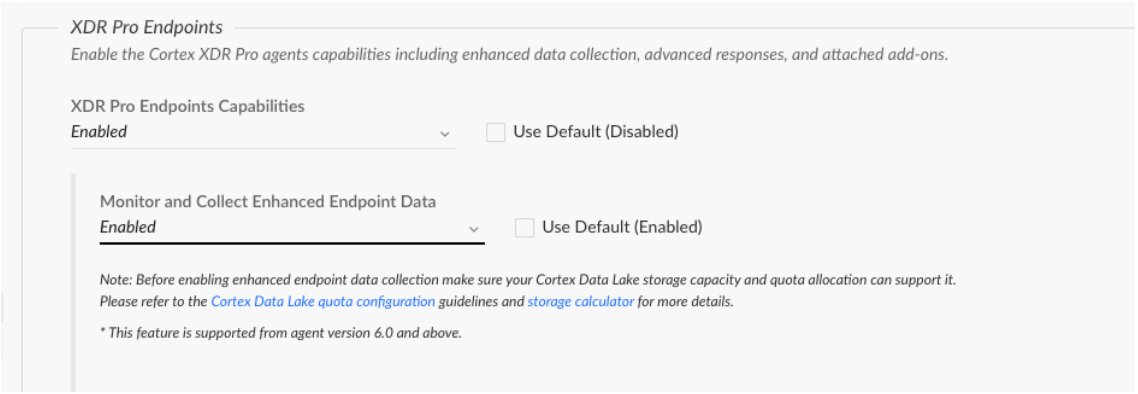

Ilustración 9. Monitor and Collect Enhanced Endpoint Data

38. La opción dentro de "**Agent Auto Update**" deberá de mantenerse con su "**ACTION MODE**" en "**Disabled**". Para ello se procede de forma homónima a la operación anterior. De este modo se mantiene en uso la versión aprobada por esta guía de seguridad, y no se llevan a cabo actualizaciones inadvertidas.

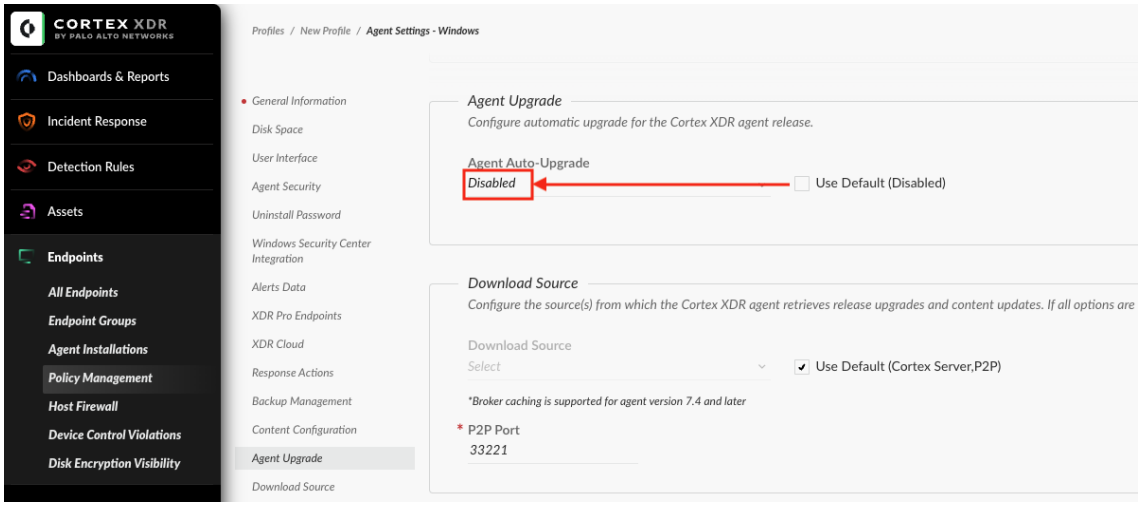

Ilustración 10. Agent Auto Upgrade

39. La nueva política deberá recibir algún nombre (por ejemplo, "Configuración LINCE"). Una vez asignado un nombre bajo "**General Information**", se podrá crear la nueva política pulsando "**Create**".

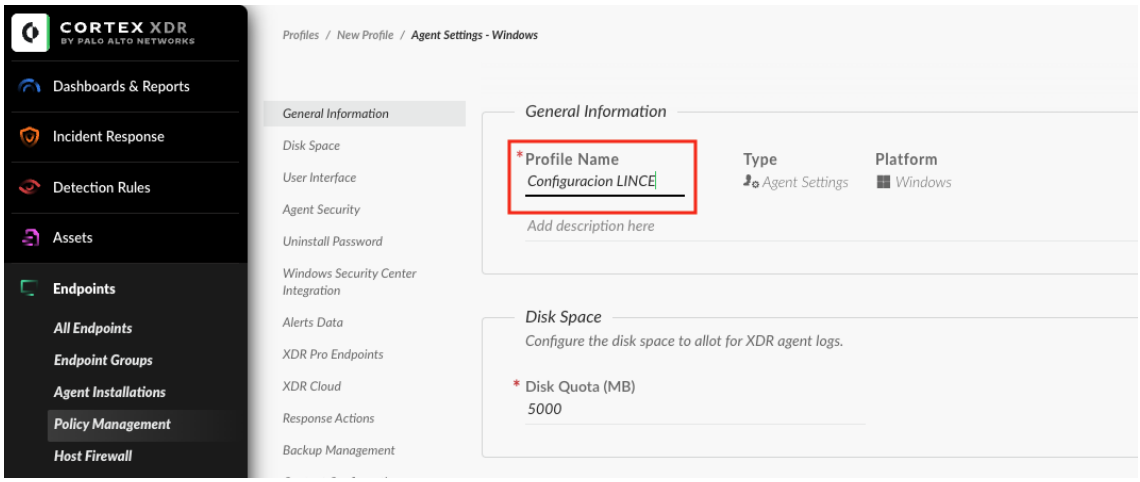

Ilustración 11. General Information

6.1.1.2 ASOCIACIÓN DE PERFIL A POLÍTICA

***NOTA**: Se deberá de crear un perfil por cada uno de los Sistemas Operativos de destino donde estará operativo el agente. Por ejemplo, si se hace uso de los agentes de Windows y Mac, estos pasos se deberán ejecutar 2 veces.*

40. Una vez creados los perfiles de políticas, es necesario ligarlos a las políticas correspondientes, para que las configuraciones se apliquen en los agentes. Para ello, se deberá hacer clic derecho en la nueva política creada en el punto anterior (verificando la plataforma, particularmente si se han creado ya políticas para otros Sistemas Operativos), y seleccionar la opción "**Create a new policy rule using this profile**".

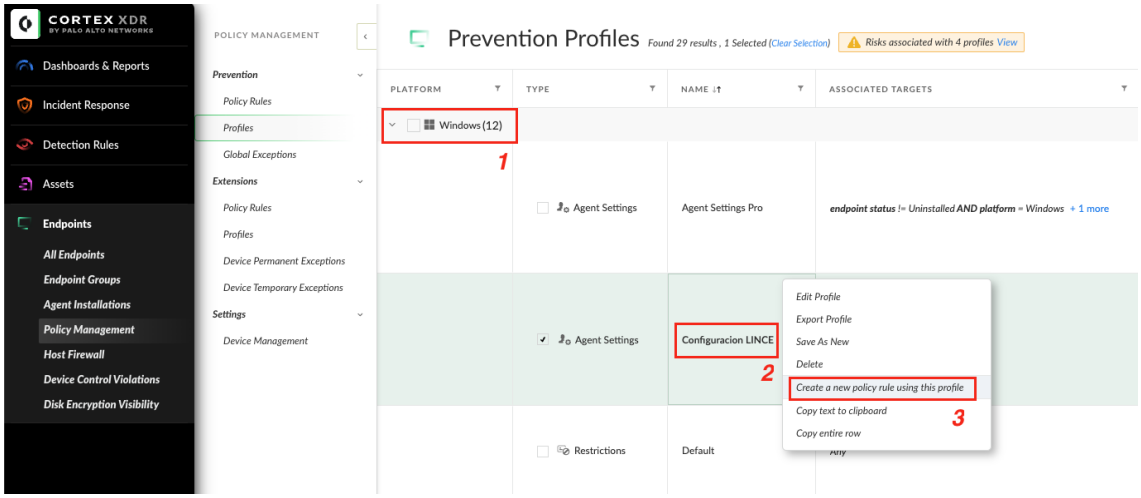

Ilustración 12. Prevention Profiles

41. En el menú de creación de política, es necesario proveer de un nombre a la política (por ejemplo, “Política LINCE”). Antes de continuar, es necesario verificar que las opciones de agente muestran la configuración creada en el punto anterior, en el ejemplo identificado como “Configuración LINCE”.

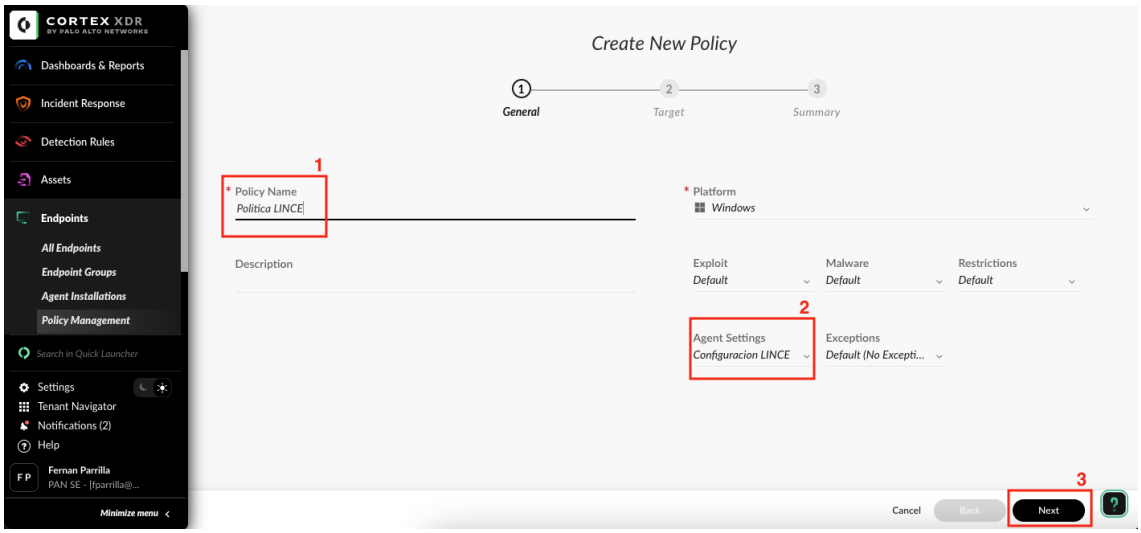

Ilustración 13. Create New Policy

42. En la siguiente pantalla, es posible que o bien se muestren los endpoints ya configurados (si estos pasos se están siguiendo después de incluir agentes en los equipos), o bien se muestre vacía. En cualquier caso, seleccionar “**Next**” sin alterar el filtro.

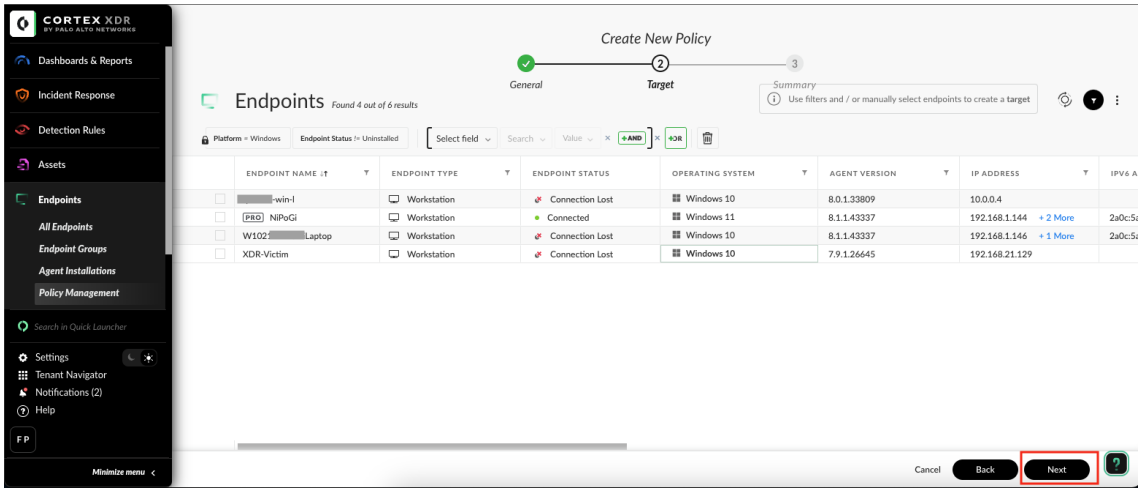

Ilustración 14. Endpoints target

43. De esta forma, el filtro por defecto seleccionará todos los endpoints para el Sistema Operativo seleccionado. En la última pantalla se podrá revisar de nuevo la configuración aplicada, que debería ser similar a la imagen mostrada abajo (si bien la cantidad de endpoints afectados será distinta). A continuación, pulsar "**Done**" para finalizar la creación.

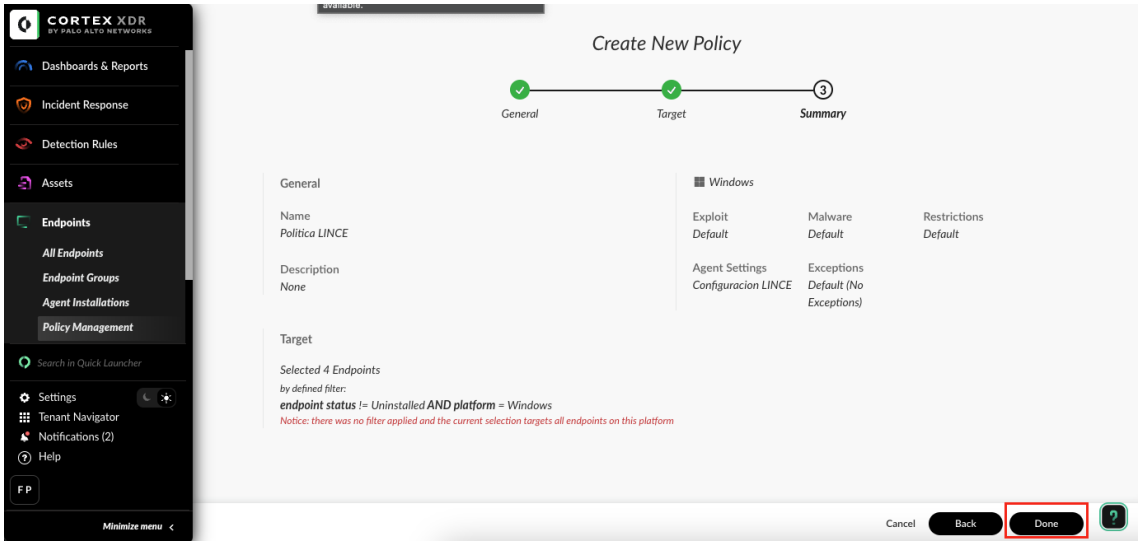

Ilustración 15. Resumen de la política a aplicar

44. Se podrá verificar entonces en el siguiente menú el que la regla ha sido creada con éxito. Se debe comprobar que la política tiene el mayor grado de precedencia (para que esta sea siempre aplicada), arrastrándola si fuera necesario hasta la primera posición en la lista. El sistema solicitará que la política se guarde para que esta se active. Para ello, haga clic en el botón "**Save**":

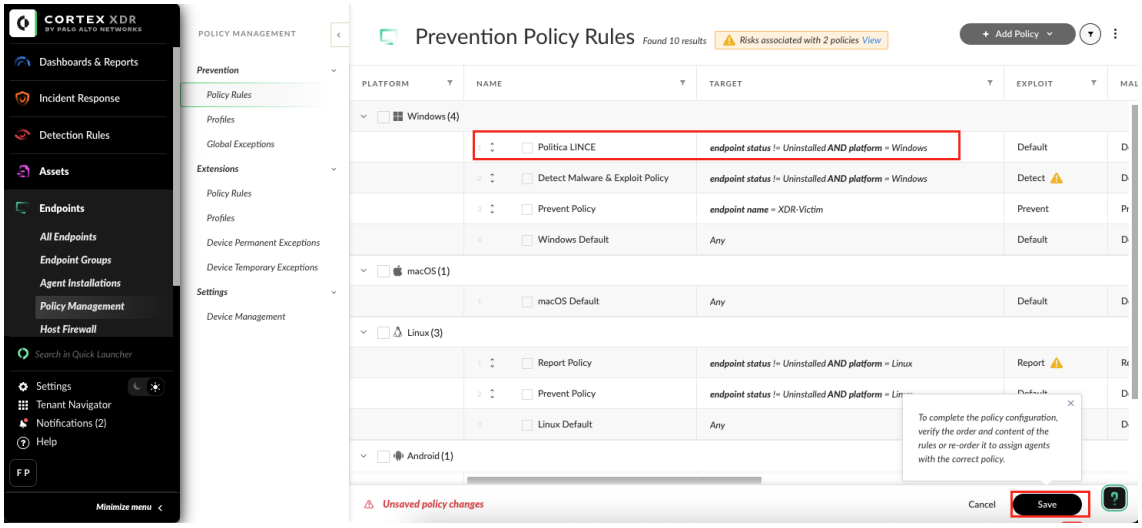

Ilustración 16. Prevention Policy Rules

45. El mensaje de "Unsaved policy changes" desaparecerá, y se mostrará un texto indicando que el cambio ha tenido éxito cerca del encabezado de la página.

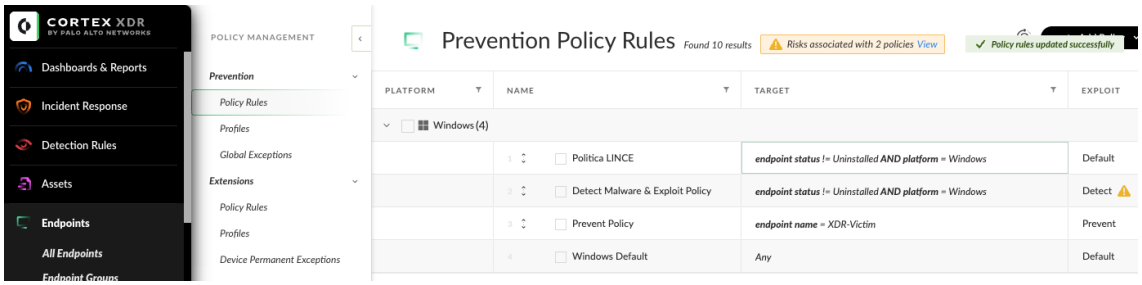

Ilustración 17. Policy Rules Updated Successfully

6.2 AUTENTICACIÓN

46. Cortex XDR soporta dos mecanismos seguros de autenticación de usuarios.

    a) Mediante el portal de soporte de cliente (CSP) [REF2]. Los usuarios con los permisos adecuados en el portal de soporte de Palo Alto Networks (al menos usuario standard) y los permisos adecuados en Cortex XDR (al menos un rol asignado) podrán autenticarse en la consola de Cortex XDR.

        i. El portal de soporte de Palo Alto hace obligatorio utilizar **autenticación de factor múltiple**, que el usuario debe configurar antes de poder acceder a Cortex XDR. Los métodos soportados son:

            - Correo electrónico (no recomendado).
            - Okta Verify (recomendado).
            - Google Authenticator (recomendado).

        ii. Los métodos de segundo factor de autenticación se configuran desde https://sso.paloaltonetworks.com/enduser/setting [REF5]. Por motivos de seguridad, para acceder a las opciones de configuración de métodos de segundo factor de autenticación es necesario el usuario y la clave y MFA utilizados durante la activación del producto.

iii. Se recomienda configurar en el portal de soporte de Palo Alto los siguientes parámetros:

- **Account Management** > **Account Details**:
  - Allow Access to Palo Alto Networks Support – **Never Allow Access**
  - New User Settings – **Require Super User Approval**
  - Default Roles for New Memberships – **Standard User**

iv. Los parámetros se encuentran prefijados a la cuenta de Palo Alto Networks:

- Longitud de contraseña: 15 caracteres, máximo 72.
- Vida mínima de contraseña por cuenta: 1 día, vida máxima 365 días.
- Las últimas 10 contraseñas empleadas no pueden ser reutilizadas.
- 5 intentos incorrectos de autenticación bloquearán la cuenta.

b) Mediante SAML SSO. Es posible configurar un *identity provider* para delegar la autenticación de los usuarios al mismo.

i. El *identity provider* deberá configurarse con los siguientes requisitos:

- Longitud mínima de la contraseña: doce (12) caracteres.
- Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales. Recomendar el uso de los cuatro (4) grupos si el producto lo permite, y al menos un mínimo de tres (3) grupos.
- Número de contraseñas anteriores que no se permite utilizar: al menos, cinco (5).
- Tiempo de validez en días de las contraseñas tras el cual expiran: aproximadamente dos meses (60 días).

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

47. El único mecanismo de administración remota se realiza mediante la consola web de administración ubicada en la nube. El acceso se realizará vía https mediante navegador por los administradores de la solución.

48. El agente puede administrarse localmente por línea de comandos mediante la herramienta **Cytool** [REF6], siempre requiriendo permisos de administrador de Windows y disponiendo de una clave correspondiente.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

6.3.3 ROLES

49. Los roles incluidos en el producto se encuentran en Default PANW roles [REF7] en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com).

50. La configuración de roles se realiza según Role permissions by components [REF8] en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com).
51. Los usuarios deben ser nominales, y la asignación de roles de acuerdo a los principios de seguridad del ENS: mínimo privilegio, separación de funciones, etc.

6.3.4 CONFIGURACIÓN DE SEGURIDAD

52. Desde Cortex XDR Settings > Configurations > General > Server Settings podrán configurarse:

User Login Expiration: Número de horas tras las que la sesión del usuario expirará. Se recomienda el tiempo mínimo, 1 hora, se puede configurar entre 1 y 24 horas.

a) **Enable Auto Logout**: permite establecer un tiempo de inactividad ante el cual se cerraría la sesión del usuario. **Se puede configurar entre 1 y 24 horas**. Por defecto viene definido a 8 horas.

b) **Dashboard Expiration**: Elegir la opción “As user login expiration”.

c) **Allowed sessions**:

- **Approved Domains**: “Enabled” y definir los dominios aprobados.
- **Approved IP ranges**: “Enabled” y definir los rangos de Ips aprobados.

d) **User Expiration**: Los usuarios se desactivarán si no se loguean. Usar el parámetro “Enabled”, el tiempo por defecto es de 30 días. Puede establecerse una fecha límite de uso del usuario en el portal de soporte de Palo Alto Networks.

e) **Allowed Domains**: Introducir dominios de la organización.

53. Para más información al respecto, se recomienda consultar el siguiente enlace [REF9].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

54. Los hosts deben conectarse a la nube de Palo Alto Networks por el puerto 443. Si su entorno restringe el acceso a Internet, permita el tráfico hacia los FQDNs indicados en la tabla.
55. La conexión saliente del agente se realiza mediante conexión SSL por el puerto 443. Si se usa descifrado SSL pueden experimentarse dificultades con la conexión de los agentes con la consola con lo que se recomienda excluir de la inspección sobre los FQDNs de la tabla.

FQDN	USO
<xdr-tenant>.xdr.<region>.paloaltonetworks.com	Usado para conectar con el tenant de Cortex XDR
distributions.traps.paloaltonetworks.com	Se utiliza para la primera solicitud en el flujo de registro, donde el agente pasa el identificador de distribución y obtiene el ch-<xdr-tenant> .traps.paloaltonetworks.com de su inquilino.

wss://lrc-<region>.paloaltonetworks.com	Se utiliza en el flujo de terminal remoto.
panw-xdr-installers-prod-us.storage.googleapis.com	Se utiliza para descargar instaladores para acciones de actualización desde el servidor.
global-content-profiles-policy.storage.googleapis.com	Se utiliza para descargar actualizaciones de contenido.
panw-xdr-evr-prod-<region>.storage.googleapis.com	Se utiliza para descargar los resultados de la solicitud de veredicto ampliado en el escaneo
https://<region>-docker.pkg.dev	Se utiliza para descargar la imagen de Kubernetes desde el registro para la instalación de los agentes de Kubernetes.
dc-<xdr-tenant>.traps.paloaltonetworks.com	Se utiliza para subir datos de EDR al tenant
ch-<xdr-tenant>.traps.paloaltonetworks.com	Se utiliza para todas las demás solicitudes entre el agente y su servidor de inquilinos, incluyendo heartbeat, cargas, resultados de acciones e informes de escaneo.
api-<xdr-tenant>.xdr.<region>.paloaltonetworks.com	Se utiliza para solicitudes y respuestas API y para conectarse a los engines.
cc-<xdr-tenant>.traps.paloaltonetworks.com	Se utiliza para solicitudes de veredicto.

Tabla 2. FQDNs para permitir en perímetro

***NOTA**: **<xdr-tenant>** se refiere al nombre del subdominio definido durante la activación del producto. Mientras que **<region>** es del código de región que se ha elegido para el despliegue del tenant durante la fase de activación del producto. El ejemplo para la región de España sería "es".*

6.5 GESTIÓN DE CERTIFICADOS

56. El agente de Cortex XDR se comunica con la consola cloud mediante TLS 1.2 en adelante no permitiendo protocolos anteriores. Los certificados usados cumplen con las especificaciones de la guía CCN-STIC-807.
57. Además, para mejorar la seguridad, se puede imponer el uso de la CA raíz proporcionada por Palo Alto Networks en lugar de la del equipo local. La configuración viene detallada en el siguiente enlace, sección Windows, punto 17 - Agent Certificates.

6.6 SERVIDORES DE AUTENTICACIÓN

58. Se puede configurar SSO mediante SAML 2.0, para ello seguir Manage Single Sign-On [REF10] en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com).

6.7 SINCRONIZACIÓN

59. No es necesaria configuración de sincronización adicional entre los agentes de Cortex XDR y la consola.

6.8 ACTUALIZACIONES

60. En el enlace Upgrade Cortex XDR Agents [REF11] en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com) se describe el proceso de actualización de los agentes XDR.

6.9 AUTO-CHEQUEOS

61. Al tratarse de una solución SaaS en la nube este apartado no aplica para Cortex XDR.

6.10 ALTA DISPONIBILIDAD

62. Al tratarse de una solución SaaS en la nube este apartado no aplica para Cortex XDR.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

63. Se puede consultar los eventos que se registran, y cómo se consultan los mismos en Monitor Administrative Activity [REF12] y los distintos tipos de mensajes de log en Management Audit Log Messages [REF13] en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com).
64. Asimismo, también se recomienda consultar el apartado Log Formats [REF14], de la Guía de Administración del producto para más información.
65. **El formato** de los registros de logs es CEF RF 5425, que sigue el siguiente mapeo:

SECCIÓN	DESCRIPCIÓN
Syslog Header	<9>: PRI (considered a prioirty field)1: version number2020-03-22T07:55:07.964311Z: timestamp of when alert/log was sentcortexxdr: host name
CEF Header	HEADER/Vendor="Palo Alto Networks" (as a constant string)HEADER/Device Product="Cortex XDR" (as a constant string)HEADER/Device Version= Cortex XDR version (2.0/2.1....)HEADER/HEADER/Severity=(integer/0 - Unknown, 6 - Low, 8 - Medium, 9 - High)HEADER/Device Event Class ID="Management Audit Logs" (as a constant string)HEADER/name = type
CEF Body	suser=user end=timestamp externalId=external_id cs1Label=email (constant string) cs1=user_mail cs2Label=subtype (constant string)

SECCIÓN	DESCRIPCIÓN
	cs2=subtype cs3Label=result (constant string) cs3=result cs4Label=reason (constant string) cs4=reason msg=event_description tenantname=tenant_name tenantCDLid=tenant_id CSPaccountname=csp_id

Tabla 3 - Formato de registros de auditoría

6.11.2 ALMACENAMIENTO LOCAL

66. El agente de Cortex XDR almacena localmente eventos y logs, se puede obtener desde la consola mediante Retrieve Support Logs from an Endpoint [REF15] en la web de documentación de Palo Alto Networks (docs.paloaltonetworks.com).
67. Asimismo, se recomienda consultar la sección "Troubleshooting resources for Windows" de la Guía de Administración de Agente [REF16] en la que vienen detallados los diferentes ficheros en el que se almacena información del agente de Cortex XDR.
68. El almacenamiento en Consola es proporcionado por el proveedor de servicios en la nube, guardándose de forma cifrada. El almacenamiento en reposo de la información se lleva a cabo mediante el uso de cifrado AES-256 bits.

6.11.3 ALMACENAMIENTO REMOTO

69. En la siguiente referencia a la documentación pública se indica cómo se configura el servicio de reenvío de logs hacia un receptor syslog, Log Forwarding [REF17]

6.12 BACKUP

70. Al ser una solución en la nube, el backup y redundancia están gestionadas por la plataforma. Puede consultarse la gestión de las mismas en Cortex XDR Privacy Datasheet [REF18] y solicitar la documentación SOC2.

7 REFERENCIAS

REF1 - Documentación oficial Cortex XDR

https://docs-cortex.paloaltonetworks.com/p/XDR

REF2 - Customer Support Portal

https://support.paloaltonetworks.com

REF3 - Activación del Producto

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Step-1-Activate-Cortex-XDR

REF4 - Creación de paquete de Instalación Windows

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Create-an-agent-installation-package

REF5 - Configuración 2FA

https://sso.paloaltonetworks.com/enduser/settings

REF6 - Cytool (Herramienta de administración de agente por línea de comandos)

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/9.0/Cortex-XDR-Agent-Administrator-Guide/Cytool-for-Windows

REF7 – Roles

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Default-PANW-roles

REF8 - Roles por componente

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Role-permissions-by-components

REF9 - Configuración de seguridad de la consola

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Configure-security-settings

REF10 - Configuración de SSO

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Authenticate-users-using-SSO

REF11 - Actualización de agente

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Upgrade-Cortex-XDR-agents

REF12 - Eventos de Auditoría de Gestión

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Monitor-administrative-activity

REF13 - Tipos de eventos de Auditoría de Gestión

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Management-audit-log-messages#

REF14 - Formatos de logs

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Log-formats

REF15 - Generar un fichero de soporte

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Retrieve-support-logs-from-an-endpoint

REF16 - Guía de Administración de agente

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/9.0/Cortex-XDR-Agent-Administrator-Guide/Cortex-XDR-agent-for-Windows

REF17 - Reenvío de logs

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-3.x-Documentation/Log-forwarding

REF18 - Datasheet de Privacidad

https://www.paloaltonetworks.com/resources/datasheets/cortex-xdr-privacy

REF19 – Matriz de compatibilidad del agente Cortex XDR

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Compatibility-Matrix/Mac

REF20 - Catálogo de Productos y Servicios TIC (CPSTIC)

https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

BIOC	Behavioral Indicators Of Compromise – Indicadores de Compromiso por comportamiento
BTP	Behavioral Threat Protection – Protección de Amenazas por Comportamiento
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
ENS	Esquema Nacional de Seguridad
EPP	Endpoint Protection Platform – Plataforma de protección del Endpoint
EDR	Endpoint Detection and Response – Detección y respuesta del Endpoint
FQDN	Full Qualified Domain Name
SAAS	Software as a Service
UEBA	Análisis de Comportamiento de Usuarios y Entidades
XDR	eXtended Detection and Response – Detección y respuesta Extendidos
XSIAM	eXtended Security Intelligence & Automation Management