Guía de Seguridad de las TIC
CCN-STIC 1018

Procedimiento de Empleo Seguro
Check Point Infinity Portal



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO Y ALCANCE 4
3 ORGANIZACIÓN DEL DOCUMENTO 5
4 FASE PREVIA A LA INSTALACIÓN 6
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 ENTORNO DE INSTALACIÓN SEGURO 6
4.3 REGISTRO Y LICENCIAS 6
4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 10
6 FASE DE CONFIGURACIÓN 12
6.1 MODO DE OPERACIÓN SEGURO 12
6.2 AUTENTICACIÓN 12
6.2.1 PRIMER INICIO DE SESIÓN 13
6.3 ADMINISTRACIÓN DEL PRODUCTO 14
6.3.1 ADMINISTRACIÓN REMOTA 14
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 18
6.3.3 VISUALIZACIÓN DE LA INFORMACIÓN DEL USUARIO 18
6.3.4 AGREGAR O ELIMINAR COLUMNAS DE LA TABLA 19
6.3.5 FILTRAR LA TABLA 19
6.3.6 EXPORTAR LA INFORMACIÓN DE LA TABLA 19
6.3.7 AGREGAR CUENTAS DE USUARIO 19
6.3.8 EDITAR CUENTAS DE USUARIO 20
6.3.9 ROLES GLOBALES 21
6.3.10 CONFIGURACIÓN DE LA POLÍTICA SEGURA DE CONTRASEÑAS 21
6.3.11 CREACIÓN DE GRUPOS DE GESTIÓN 22
6.4 SERVIDORES DE AUTENTICACIÓN 24
6.5 SINCRONIZACIÓN 25
6.6 ACTUALIZACIONES 25
6.7 ALTA DISPONIBILIDAD 25
6.8 AUDITORÍA 26
6.8.1 REGISTRO DE EVENTOS 26
6.8.2 ALMACENAMIENTO REMOTO 26
6.9 BACKUP 26
REFERENCIAS 27
7 ABREVIATURAS 28

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Entrada al Infinity Portal 6
Ilustración 2. Selección de Contratos 7
Ilustración 3. Menú User Center 7
Ilustración 4. Selección User Center 8
Ilustración 5. Esquema Check Point Infinity Portal 8
Ilustración 6. Datos necesario para alta en Infinity Portal 10
Ilustración 7. Mensaje de Confirmación 10
Ilustración 8. Ejemplo de email de invitación 11
Ilustración 9. Primer login en Infinity Portal 11
Ilustración 10. Menú de ajustes 12
Ilustración 11. Login en Infinity Portal 12
Ilustración 12. Selección de región. 13
Ilustración 13. Selección de usuario 13
Ilustración 14. Validación segundo factor 14
Ilustración 15. Productos Infinity Portal 14
Ilustración 16. Propiedades de la cuenta 14
Ilustración 17. Detalles de la cuenta 15
Ilustración 18. Configuración de proveedor de identidades 15
Ilustración 19. Configuración de permisos 15
Ilustración 20. Menú de grupos 16
Ilustración 21. Menú auditoría 16
Ilustración 22. Menú de licencias y contratos 17
Ilustración 23. Menú uso de licencias 17
Ilustración 24. Menú de claves de API 18
Ilustración 25. Menú envio de logs 18
Ilustración 26. Menú datos de usuarios 20
Ilustración 27. Edición cuentas de usuario 21
Ilustración 28. Opciones de seguridad de contraseña 22
Ilustración 29. Detalle tiempo de sesión 22
Ilustración 30. Menú grupos de gestión 22
Ilustración 31. Configuración nombre del grupo de gestión 23
Ilustración 32. Menú añadir administradores a grupo 23
Ilustración 33. Asignación de roles de gestión 24
Ilustración 34. Tabla de capacidades 25
Ilustración 35. URL de monitorización de recursos 25
Ilustración 36. Opciones del Infinity Portal 26
Ilustración 37. Vista de eventos del portal 26

ÍNDICE DE TABLAS

Tabla 1. Tipos de Roles Globales 21

1 INTRODUCCIÓN

La plataforma **Infinity Portal** constituye la solución de gestión en modalidad Software como Servicio (SaaS) orientada a la administración unificada y centralizada de los servicios de seguridad de Check Point.

Conforme a las directrices de seguridad recogidas en la presente guía CPSTIC / Guía CCN-STIC, esta plataforma actúa como punto único de control para optimizar la gobernanza, robustecer la postura de ciberseguridad corporativa y garantizar la trazabilidad operacional sobre el conjunto de activos de la organización.

El personal de administración con privilegios operará Check Point Portal bajo el principio de mínimo privilegio y autenticación reforzada, disponiendo de las siguientes capacidades funcionales:

- **Gestión centralizada de la seguridad**: Consola unificada para la definición, orquestación y aplicación homogénea de directivas y políticas de seguridad transversalmente entre los diferentes módulos y servicios desplegados.
- **Despliegue y aprovisionamiento seguro**: Mecanismo automatizado que permite a los administradores propagar de forma controlada y ágil nuevas configuraciones y políticas de seguridad hacia todos los dispositivos y nodos conectados.
- **Monitorización y visibilidad en tiempo real:** Supervisión continua del estado de la seguridad que proporciona telemetría inmediata ante alertas e incidentes, facilitando una respuesta temprana y mitigando el riesgo de brechas de seguridad o accesos no autorizados.
- **Analítica, auditoría e informes**: Herramientas avanzadas de análisis y generación de informes de rendimiento y eventos, destinadas a evaluar la eficacia de los controles implementados e identificar vectores de mejora en la infraestructura.

2 OBJETO Y ALCANCE

El objeto del presente Procedimiento de Empleo Seguro (PES) es definir las directrices de configuración, operación y administración segura aplicables **exclusivamente a la plataforma base Infinity Portal** como consola SaaS de gestión y orquestación centralizada. Por tanto, el alcance técnico de este documento queda circunscrito de forma estricta a la gobernanza del propio portal, sus mecanismos de autenticación, control de accesos, gestión de identidades y pistas de auditoría de la plataforma administrativa.

Quedan expresamente excluidos del alcance del presente PES todos y cada uno de los servicios, productos y cargas de trabajo gestionados a través de él (tales como Quantum, Harmony, CloudGuard o cualquier otra solución satélite), debiendo regirse el despliegue y la operación de dichas aplicaciones por sus correspondientes Procedimientos de Empleo Seguro y guías de configuración específicas del catálogo CPSTIC / CCN-STIC.

El producto **Check Point Infinity Portal** ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF7].

3 ORGANIZACIÓN DEL DOCUMENTO

El presente documento está organizado de la siguiente manera:

a) Apartado 0. 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 0. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Al ser un servicio SaaS, la "entrega" se realiza mediante la creación de un Tenant en la infraestructura de Check Point.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Dado que el portal reside en la nube, el entorno de instalación seguro se refiere a la **Workstation de gestión**. Esta debe estar ubicada en una red controlada y el acceso físico y lógico al equipo debe estar restringido a personal autorizado.

4.3 REGISTRO Y LICENCIAS

El registro del tenant y la activación de licencias se detallan en la documentación oficial de Check Point (disponible en Support Center [REF7]). Una vez adquiridas las licencias y dado de alta el tenant, hay que seguir los siguientes pasos para sincronizar las licencias con el portal:

- Acceder al Infinity Portal [REF5] .
- En portal.checkpoint.com, al lado del nombre del tenant, hay una rueda que nos permite acceder a la configuración general del tenant.

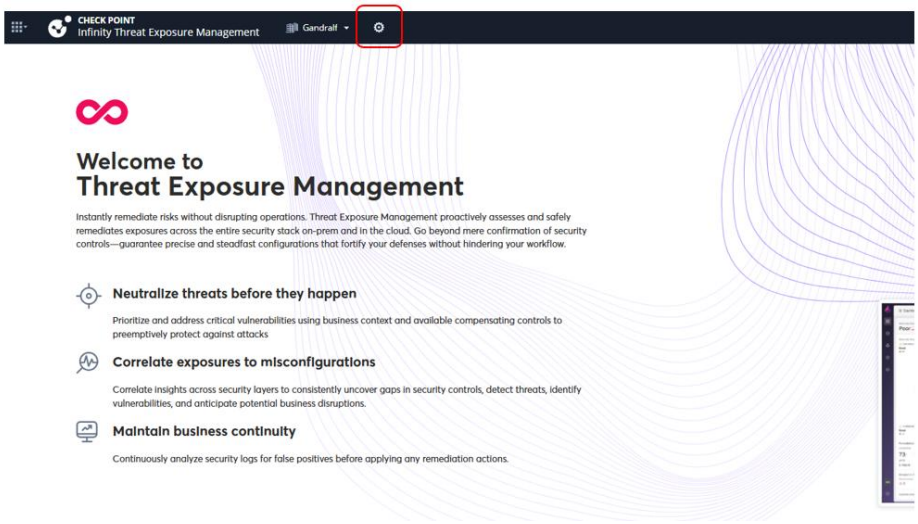


Ilustración 1. Entrada al Infinity Portal

- Seleccionar la opción Services & Contracts.

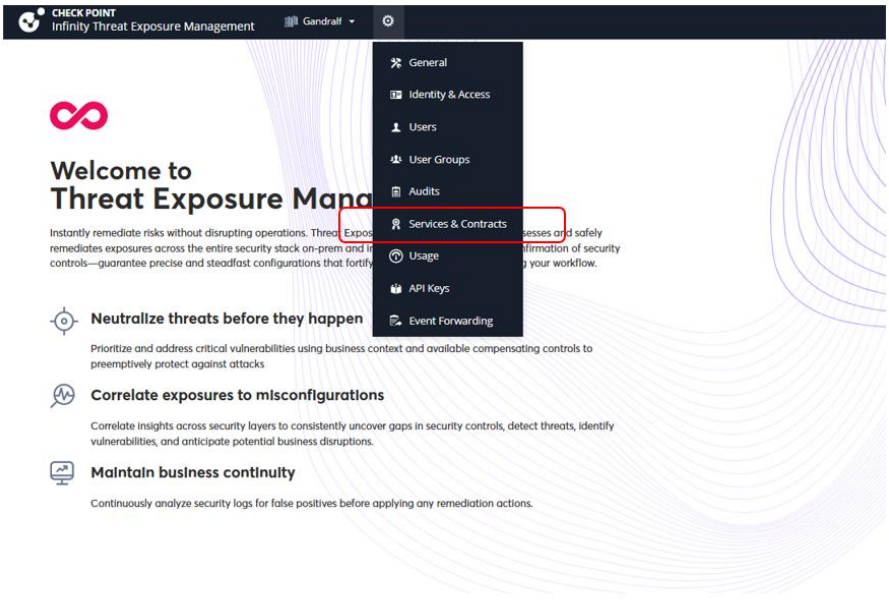


Ilustración 2. Selección de Contratos

- En esta pantalla por un lado veremos las licencias que están activas y el servicio al que están adjuntadas. Para añadir una cuenta nueva hay que seleccionar en "Manage Accounts – Attach UC Account".

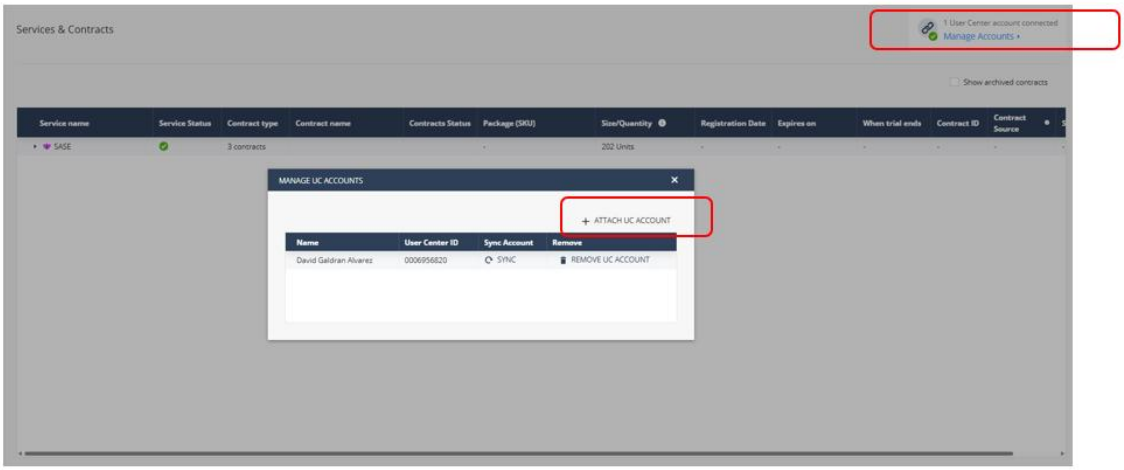


Ilustración 3. Menú User Center

- Introducimos el usuario y contraseña de nuestra cuenta de User Center, (el cual se recibe cuando se adquiere el producto por primera vez). En el User Center es donde se almacenan las licencias y seleccionamos la cuenta en concreto:

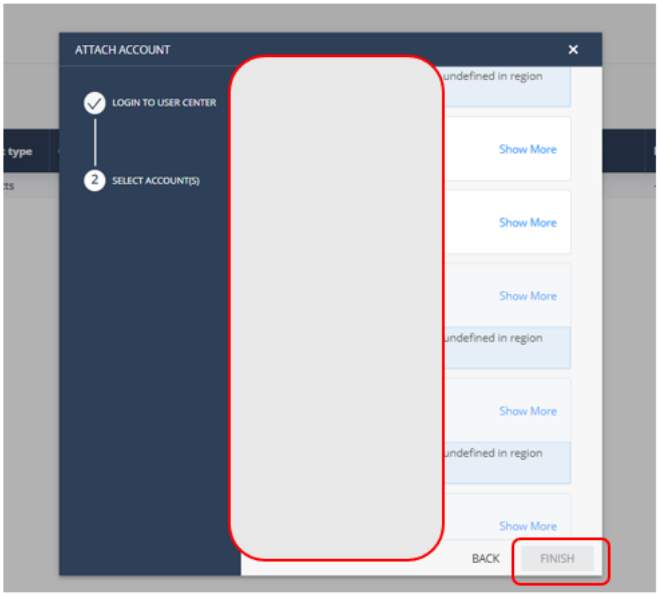


Ilustración 4. Selección User Center

- Una vez hecho esto, las licencias aparecerán en el portal. Es importante tener en cuenta que desde el momento en que sincronicemos una cuenta de User Center [REF7] con el portal, todas las licencias que se vayan añadiendo a ese User Center se sincronizarán de forma automática en nuestro Infinity Portal.

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

Infinity Portal es un servicio SaaS que unifica los distintos entornos de administración de las soluciones de Check Point. Para acceder al servicio se necesita un navegador web que soporte una conexión segura. El esquema de la solución es el siguiente:

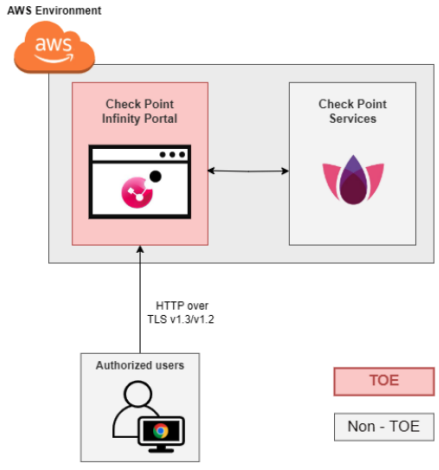


Ilustración 5. Esquema Check Point Infinity Portal

Los componentes de este entorno son:

- **Usuarios Autorizados**. Estos usuarios acceden y administran las distintas funcionalidades del portal. Dependiendo de la funcionalidad podrían acceder a los distintos servicios de Check Point que están activos en el Infinity Portal.

- **Servicios de Check Point**. Los distintos servicios de gestión que se encuentran activos en Infinity Portal para la gestión de los disintos productos como Harmony Email and Collaboration, Harmony Mobile, IoT Protect. El uso seguro de estas soluciones está fuera del scope del presente PES.

5 FASE DE INSTALACIÓN

Al ser un modelo SaaS, no hay instalación de servidor. Sin embargo, se debe configurar el acceso web mediante un navegador que soporte los estándares criptográficos requeridos por la guía CCN-STIC-807. Infinity Portal soporta los siguientes navegadores:

- Mozilla Firefox
- Google Chrome
- Apple Safari
- Opera
- Microsoft Edge

Los pasos para crear un Infinity Portal por primera vez son los siguientes:

- Acceder a Infinity Portal [REF5] y seleccionar “Don’t have an account? Register here”.
- Rellenar los campos necesarios. IMPORTANTE, para asegurar la residencia de datos en espacio europeo, es necesario seleccionar debajo del país la zona EU perteneciente a Europa.

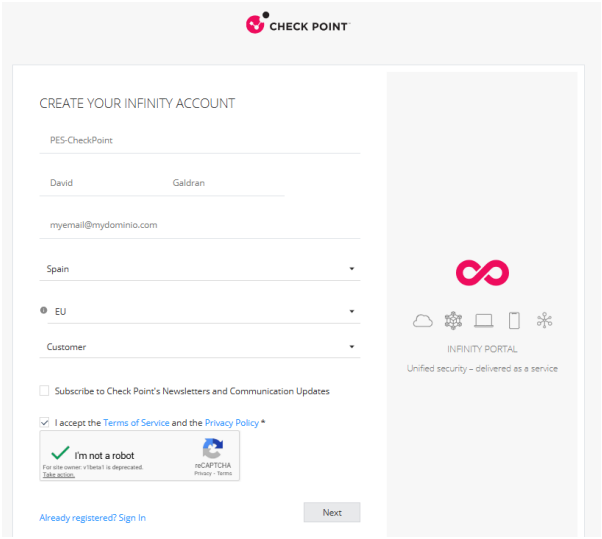


Ilustración 6. Datos necesario para alta en Infinity Portal

- IMPORTANTE. El producto no permite hacer enrollment con cuentas tipo @gmail. Una vez se haya creado el tenant, nos saldrá un mensaje indicando que el tenant se ha creado de forma satisfactoria.

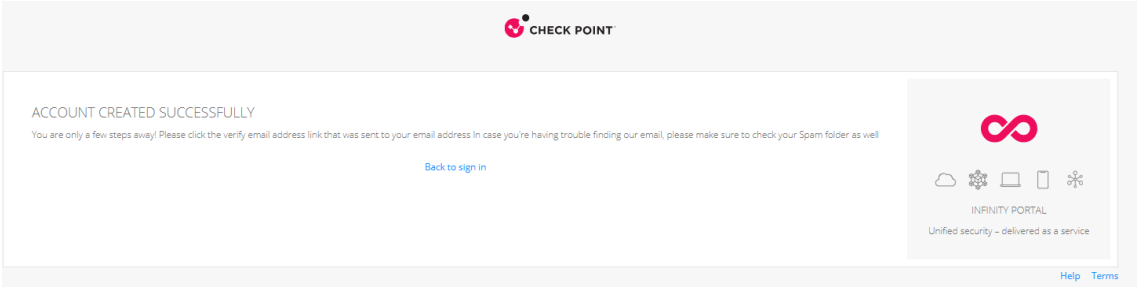


Ilustración 7. Mensaje de Confirmación

- Una vez creado el tenant. Nos llegará un correo de bienvenida de la dirección do-not-reply@checkpoint.com, con la invitación al tenant. Es obligatorio hacer click en esta invitación para tener acceso al tenant que acabamos de crear:

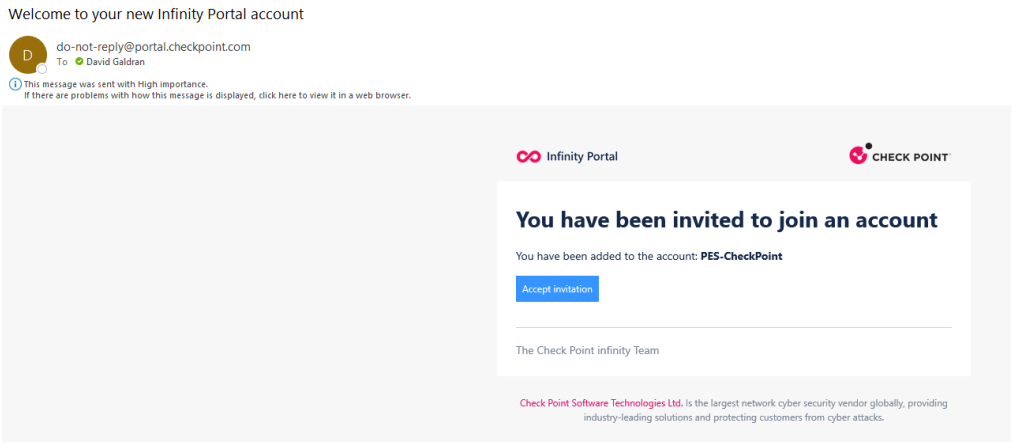


Ilustración 8. Ejemplo de email de invitación

- Nos redirigirá a la página de Infinity Portal [REF5] con el nuevo tenant que hemos creado. Nos autenticamos con nuestras credenciales y ya podremos acceder:

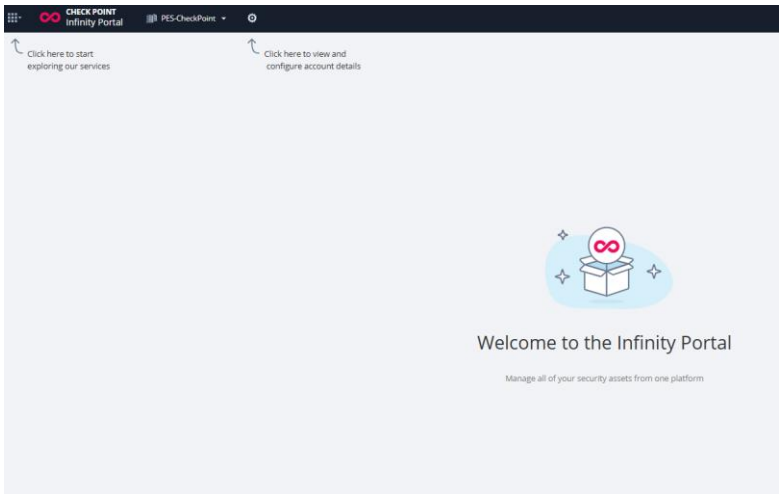


Ilustración 9. Primer login en Infinity Portal

No obstante, se dispone de un video explicativo [REF4] para la creación de portal en el apartado de Referencias.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Una cuenta de Infinity Portal es necesaria para acceder a las distintas plataformas de gestión SaaS de los productos de Check Point. Por defecto el usuario que crea el portal por primera vez recibe los permisos de "primary administrator". Este rol que a posteriori se puede delegar en otro usuario tiene permisos especiales que permite:

- Administrar entidades.
- Dar accesos a nuevos administradores.
- Redirección de logs.

Todas y cada una de estas acciones se encuentran en el apartado de ajustes al cual se accede haciendo click con el ratón en la imagen con forma de rueda que se encuentra a la derecha del nombre.

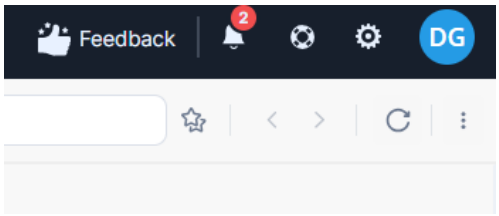


Ilustración 10. Menú de ajustes

6.2 AUTENTICACIÓN

El método preferido para iniciar sesión en el Portal Infinity es mediante la autenticación SSO. Si este método no está disponible, puede iniciar sesión con:

- nombre de usuario y contraseña.
- Credenciales de GitHub.

Para iniciar sesión en la cuenta:

- Acceda a Infinity Portal [REF5] e introduzca la dirección de correo electrónico.

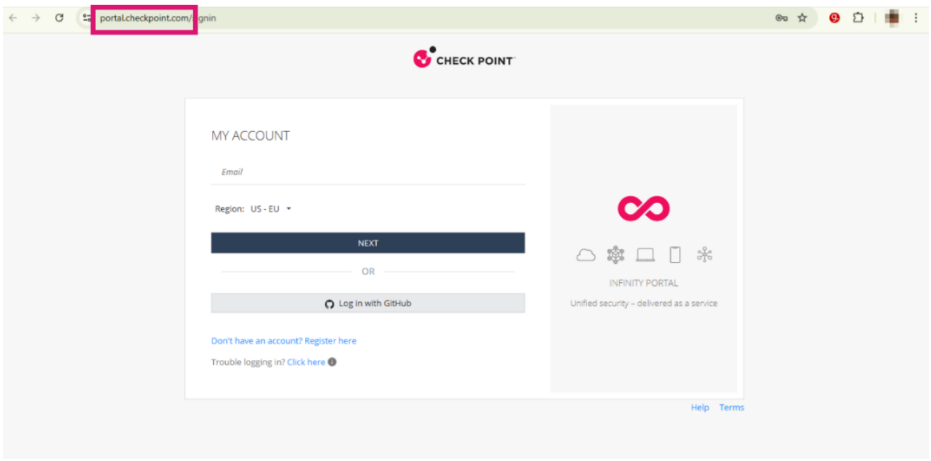


Ilustración 11. Login en Infinity Portal

- Seleccione la región que desea utilizar.

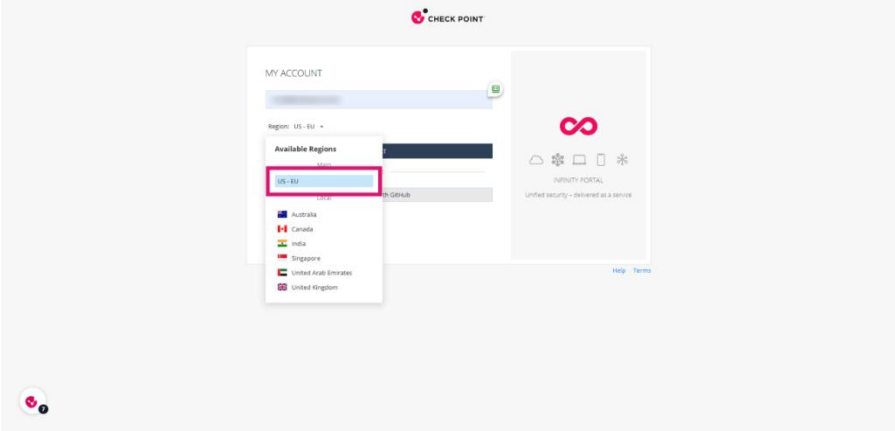


Ilustración 12. Selección de región.

- Haga clic en Siguiente.

Para iniciar sesión con GitHub:

- Acceda al Infinity Portal [REF5] e introduzca su dirección de correo electrónico.
- Seleccione la región que desea utilizar.
- Haga clic en Iniciar sesión con GitHub.
- Se abre la página de inicio de sesión de GitHub.
- Introduzca sus credenciales de GitHub:
  - Introduzca su nombre de usuario de GitHub o su dirección de correo electrónico, y luego introduzca su contraseña.
  - Como alternativa, haga clic en Continuar con Google para usar su cuenta de Google corporativa (de trabajo o de la escuela).
- Haga clic en Iniciar sesión.

6.2.1 PRIMER INICIO DE SESIÓN

En el primer inicio de sesión es recomendable activar el MFA para el usuario. Antes de comenzar el procedimiento es obligatorio revisar que el número de teléfono del administrador que se creó en el portal es correcto. El procedimiento de activación del MFA es el siguiente:

- Descargue, desde los Marketplace oficiales del SSOO del terminal móvil, una de estas aplicaciones de autenticación en tu teléfono móvil:
  - Google Authenticator
  - Microsoft Authenticator
  - Authy
- En el Portal Infinity, abra la página de Configuración del Perfil. En la esquina superior derecha:
- Haga clic en la flecha hacia abajo junto al nombre de usuario > Configuración del perfil. Se abre la ventana de Configuración del perfil.



Ilustración 13. Selección de usuario

- Activar el interruptor “Enforce Multi-Factor Authenticator” a ON. Se abre el asistente de configuración, generándose un código QR para añadir la configuración MFA a la aplicación seleccionada.
- Haga clic en Terminar para cerrar el asistente. Se mostrará en verde que el usuario tiene activado la autenticación MFA:

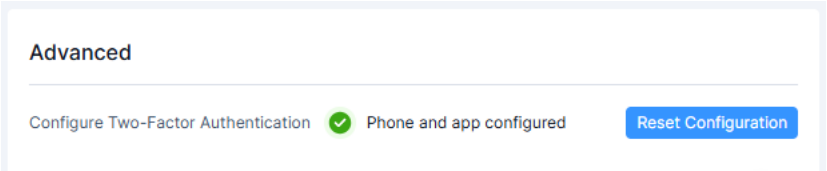


Ilustración 14. Validación segundo factor

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN REMOTA

Una vez autenticados en la plataforma Infinity Portal [REF5] podemos acceder a la activación de los distintos servicios:

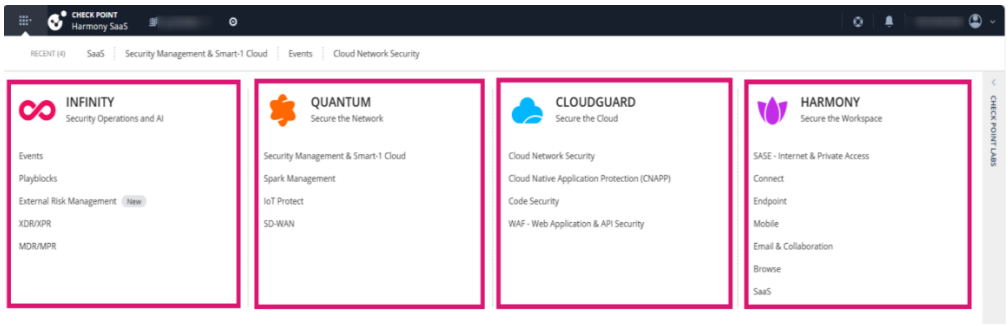


Ilustración 15. Productos Infinity Portal

Pulsando en la rueda situada a la derecha del nombre del portal accederemos a las propiedades de la cuenta.

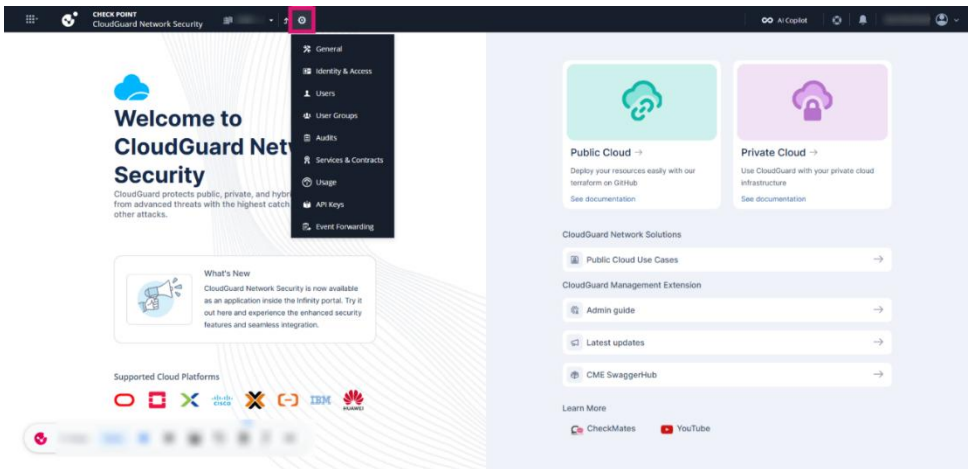


Ilustración 16. Propiedades de la cuenta

En los settings generales se pueden editar los detalles de la cuenta, dar acceso a soporte para realizar troubleshooting o bien eliminar la cuenta:

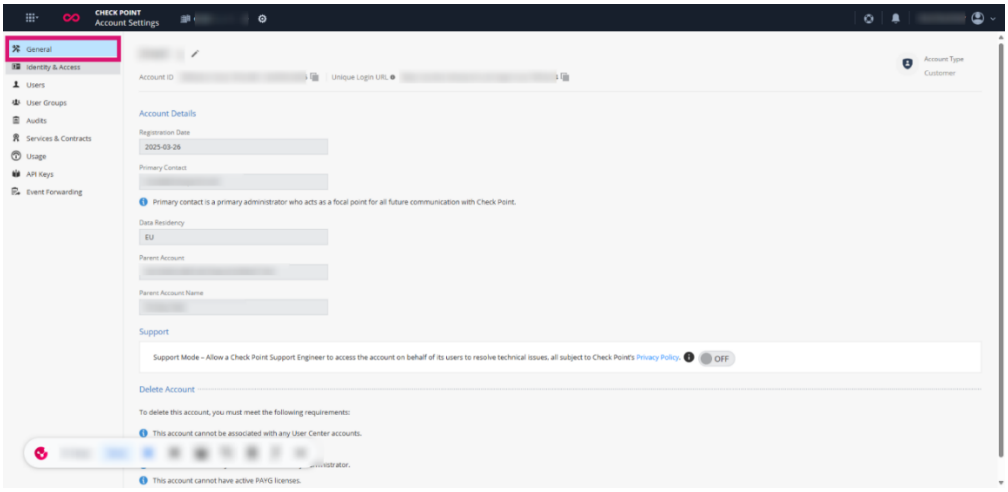


Ilustración 17. Detalles de la cuenta

En la pestaña Identity and Access se puede configurar el mecanismo de SSO con terceras partes, la frecuencia de login, timeout y la validación multifactor.

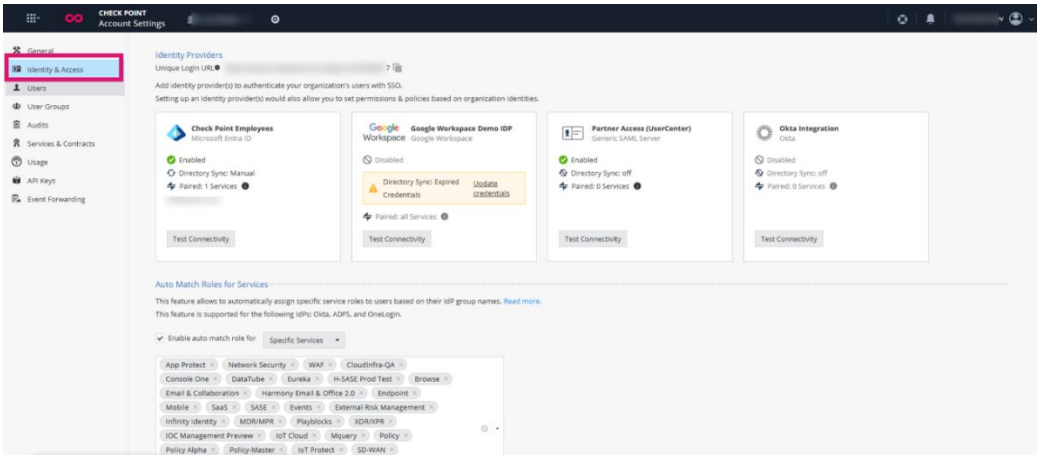


Ilustración 18. Configuración de proveedor de identidades

En la pestaña usuarios, se puede crear, editar y eliminar los perfiles de los usuarios de Infinity Portal. Esta opción sólo está disponible para los administradores con el rol de "User Admin".

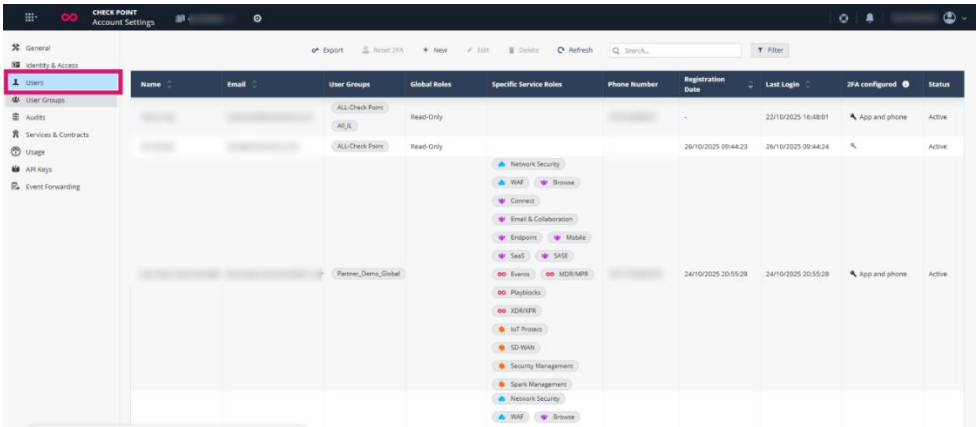


Ilustración 19. Configuración de permisos

En la pestaña User Groups, se pueden crear, editar y borrar los grupos de usuario, esta sección solo es visible para usuarios con el rol “User Admin”.

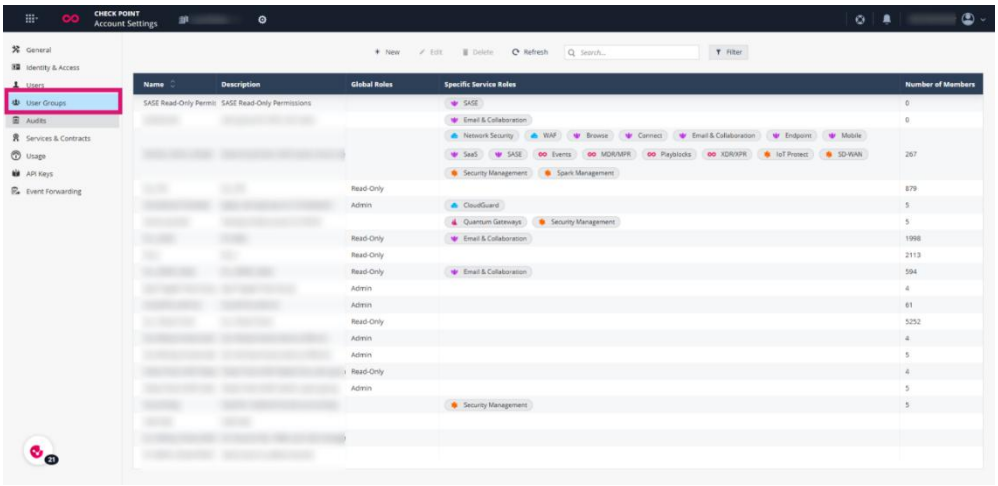


Ilustración 20. Menú de grupos

La sección Audits contiene los logs de los usuarios y su actividad.

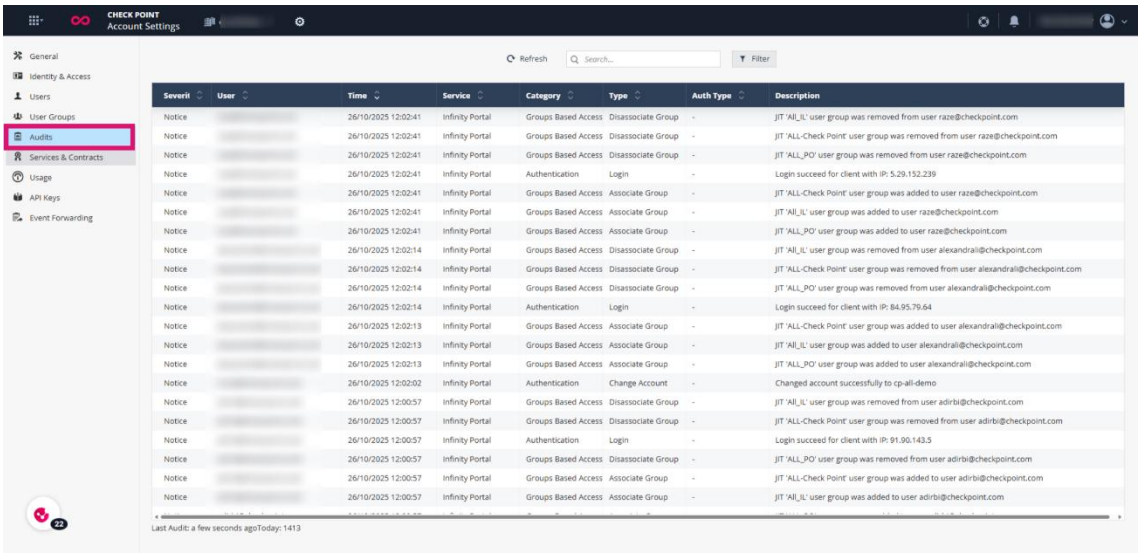


Ilustración 21. Menú auditoría

La sección Services & Contracts es donde se gestionan las cuentas de usercenter que contienen las licencias de los productos que se han desplegado en Infinity Portal.

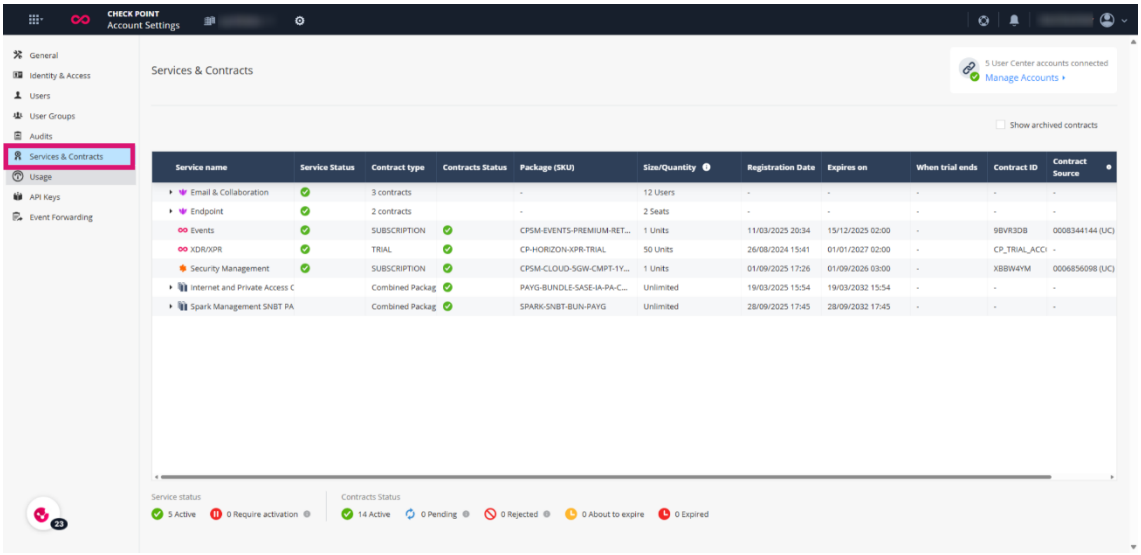


Ilustración 22. Menú de licencias y contratos

En la pestaña Usage se dispone de un informe de uso de licencias de todos los productos.

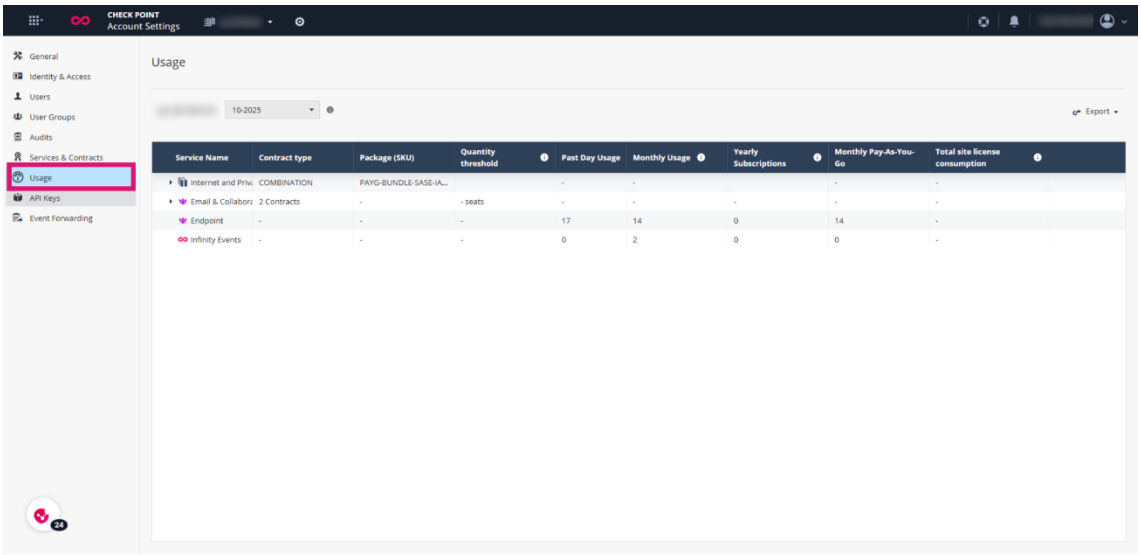


Ilustración 23. Menú uso de licencias

En la pestaña API Keys es donde se configuran las API para las distintas automatizaciones con aplicaciones de terceros. Cada aplicación recibe desde aquí su propia API Key.

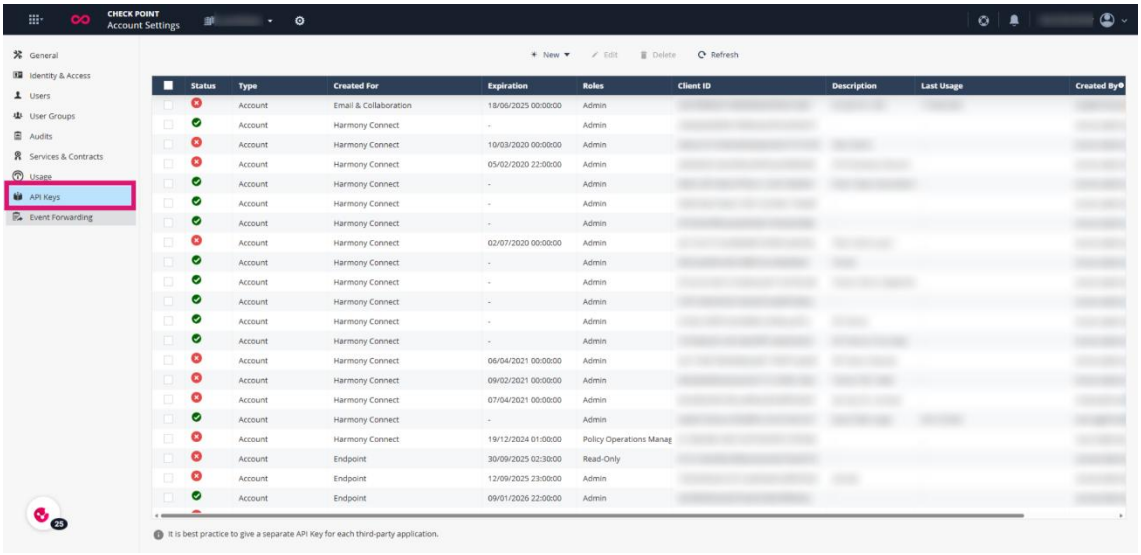


Ilustración 24. Menú de claves de API

En la última opción "Event Forwarding" se configura la exportación de los logs a los distintos SIEM.

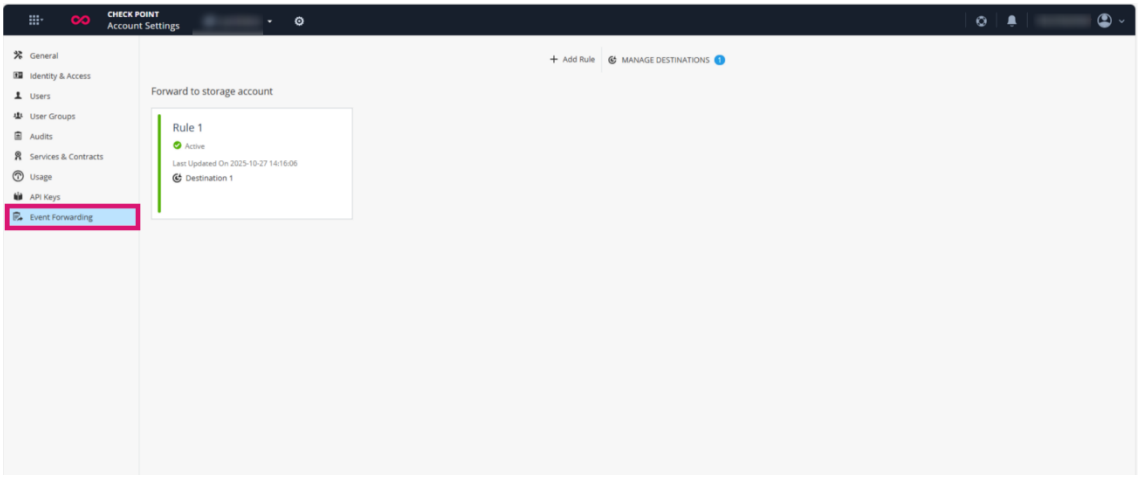


Ilustración 25. Menú envio de logs

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

El manual de configuración de administradores viene detallado en el apartado Account Settings, Users, del Manual de administrador de Infinity Portal [REF 8].

6.3.3 VISUALIZACIÓN DE LA INFORMACIÓN DEL USUARIO

Muestra la información del usuario

- Ir a Configuración > Usuarios.
- Para ver la información de usuario actualizada, haga clic en Actualizar.

6.3.4 AGREGAR O ELIMINAR COLUMNAS DE LA TABLA

- Haga clic con el botón derecho en la primera fila de la tabla que contiene los nombres de las columnas.
- Se abre una lista con los nombres de las columnas.
- Seleccione las columnas que desea mostrar en la tabla.
- Solo las columnas seleccionadas aparecen en la tabla.

6.3.5 FILTRAR LA TABLA

- En el campo de búsqueda, haga clic en Filtrar.
- Se abre el panel de filtros.
- Para encontrar usuarios específicos, introduzca estos datos:
  - Nombre
  - Correo electrónico
  - etc.
- Para borrar el filtro, haga clic en Borrar todo.

6.3.6 EXPORTAR LA INFORMACIÓN DE LA TABLA

- Haga clic en Exportar.
- Tu navegador web descarga un archivo ZIP.
- Una vez finalizada la descarga, guarde el archivo en su ordenador y extraiga el contenido en un archivo CSV.
- Abra el archivo CSV en una aplicación (por ejemplo, Microsoft Excel).

6.3.7 AGREGAR CUENTAS DE USUARIO

Puedes invitar a usuarios a la cuenta de Infinity Portal que administras. Tras invitar a un usuario, Infinity Portal le enviará una invitación por correo electrónico. Para aceptarla, el usuario deberá hacer clic en un enlace del correo. La invitación es válida durante 30 días.

Nota: Todos los campos marcados con un asterisco (*) son obligatorios.

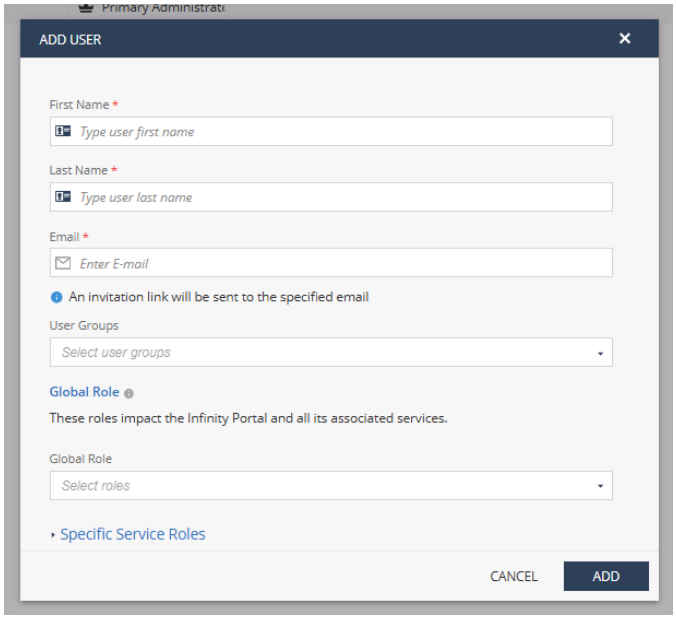


Ilustración 26. Menú datos de usuarios

Navegue hasta Opciones> Usuarios y haga clic en Nuevo en la barra de herramientas.

- En el campo Nombre, introduzca un nombre para el usuario.
- En el campo Correo electrónico, introduzca la dirección de correo electrónico del nuevo usuario.
- En el campo Grupos de usuarios, seleccione los grupos de usuarios para el nuevo usuario de la lista. Puede seleccionar varios grupos de usuarios para cada usuario.
- En el campo Roles globales, seleccione los roles para el nuevo usuario de la lista. Puede seleccionar varios roles para cada usuario.
- Seleccione los roles de servicio específicos que se asignarán al usuario.
- Haga clic en Agregar para guardar o en Cancelar para salir sin guardar el nuevo usuario.
- El usuario aparece con el estado Pendiente en la lista completa de usuarios.
- Cuando el usuario recibe la invitación por correo electrónico y hace clic en el enlace "Aceptar invitación", el Portal Infinity comprueba si se trata de un usuario nuevo o existente.

Para los nuevos usuarios, el Portal Infinity se abre con una pantalla de activación y una solicitud para establecer una nueva contraseña. La política de contraseñas se muestra en la misma página.

- El usuario introduce la contraseña, la confirma, selecciona " Acepto los Términos de servicio y la Política de privacidad" y hace clic en "Activar".
- El Portal Infinity activa al usuario.

6.3.8 EDITAR CUENTAS DE USUARIO

El procedimiento para editar una cuenta de usuario existente es el siguiente:

- Seleccione el usuario de la lista y haga clic en Editar en la barra de herramientas.

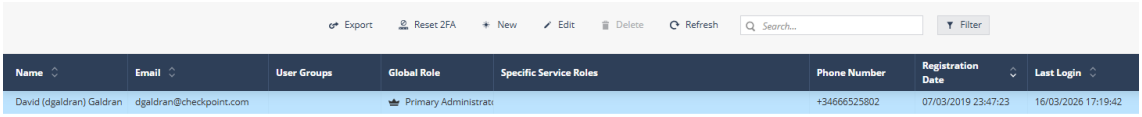


Ilustración 27. Edición cuentas de usuario

- Realice los cambios necesarios. Puede editar el nombre del usuario, el número de teléfono, la afiliación a grupos de usuarios y los roles de servicio globales y específicos.
- Haga clic en Guardar.

6.3.9 ROLES GLOBALES

Los administradores de la plataforma disponen de la posibilidad de tener asignado un Global Role el cual le asignará distintos privilegios sobre el portal.

Tabla 1. Tipos de Roles Globales

Global Role	Privilegio
Read Only	Dispondrá de permisos de solo lectura sobre el portal
User Admin	Puede ejecutar acciones de escritura y modificación sobre usuarios y grupos
Admin	Puede ejecutar acciones de escritura y modificación sobre usuarios y la cuenta.
Primary Admin	Tiene los mismos permisos que un usuario tipo Admin y además tiene permisos para modificar SSO, MFA y dar de baja la cuenta.

Los pasos para la asignación de los distintos roles a un usuario se describen en el Manual de Administración de Infinity Portal, sección Global Roles [REF9]

6.3.10 CONFIGURACIÓN DE LA POLÍTICA SEGURA DE CONTRASEÑAS

La configuración de la política de contraseñas se realiza desde el menú de opciones, Identity Access. En Password Settings, se configuran los tiempos de rotación de las contraseñas, política de reutilización y tamaño mínimo de las mismas. Para configurar la solución de acuerdo con el **ENS de nivel alto** se requiere que el valor de estos sea:

- Rotación de la contraseña: 180 días.
- Prevención de reutilización de contraseñas: últimas 5 contraseñas.
- Longitud mínima de la contraseña: 15 caracteres.

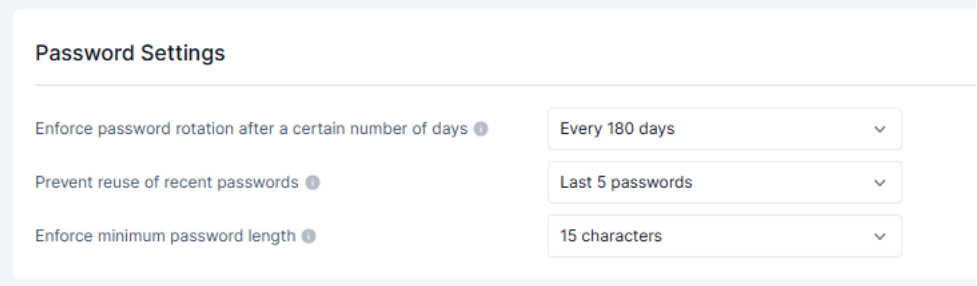


Ilustración 28. Opciones de seguridad de contraseña

En el apartado Sessions, se configura el tiempo máximo de sesión y el tiempo de desconexión por timeout

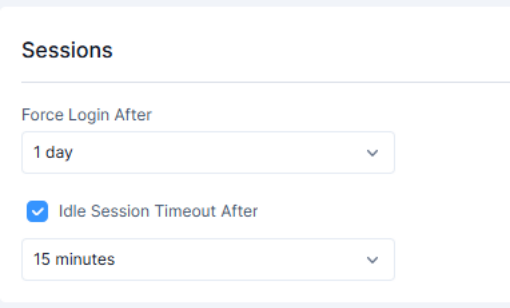


Ilustración 29. Detalle tiempo de sesión

6.3.11 CREACIÓN DE GRUPOS DE GESTIÓN

Se recomienda que la gestión de los permisos de los usuarios de administración se haga en base a grupos. Esta asignación se realiza en el menú "Opciones – User Groups":

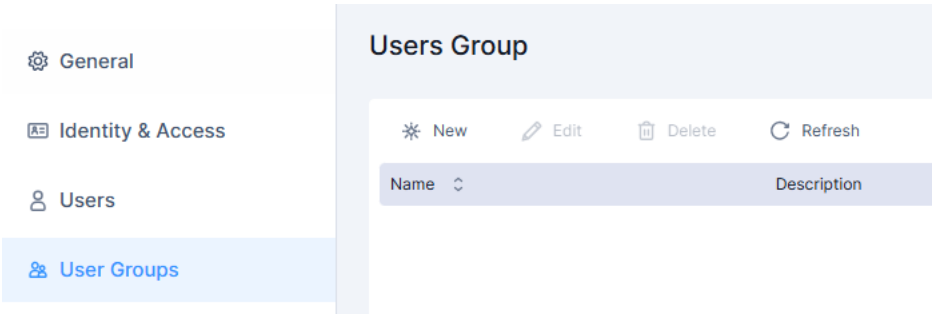


Ilustración 30. Menú grupos de gestión

En este apartado se crea el grupo y se asigna a los distintos usuarios de gestión, el procedimiento es el siguiente:

- Haga click en el botón new, se abre el wizard de configuración donde en el primer paso se debe de indicar el Nombre y la Descripción

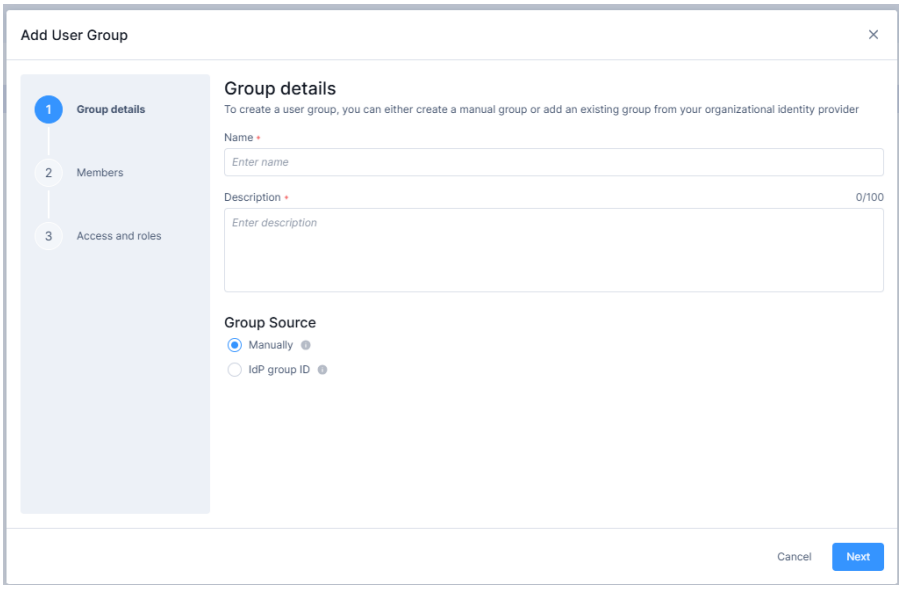


Ilustración 31. Configuración nombre del grupo de gestión

- A continuación, se eligen los Administradores que formarán parte del grupo:

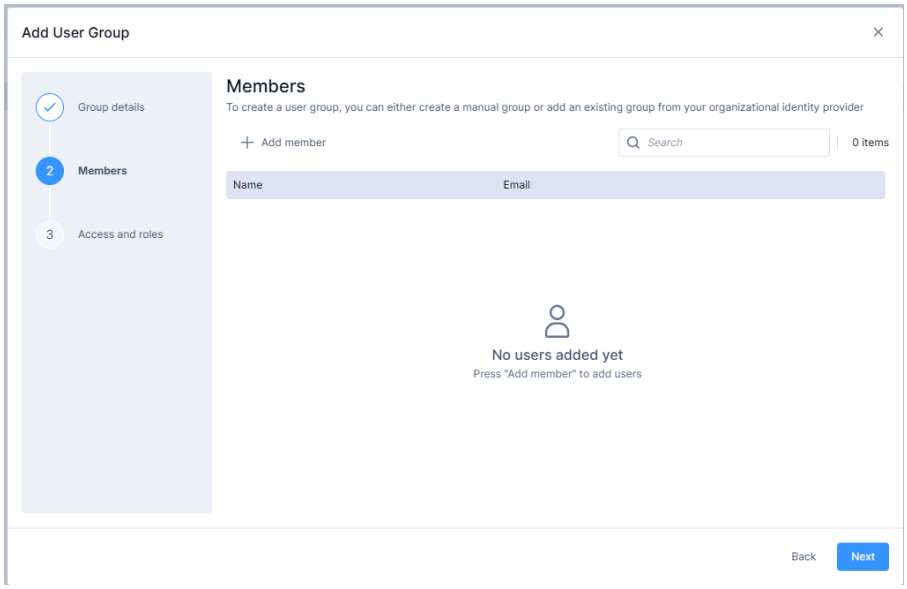


Ilustración 32. Menú añadir administradores a grupo

- Por último, se le asignan los roles correspondientes

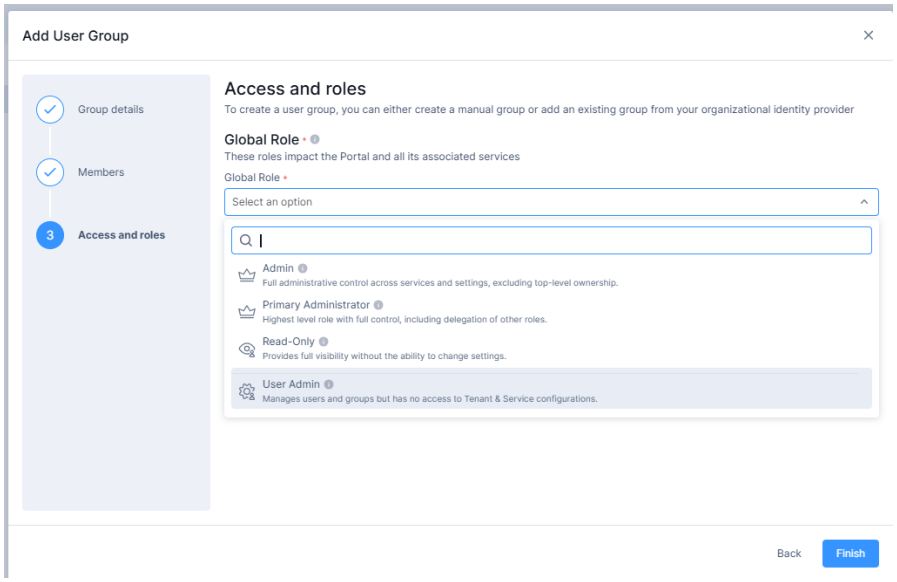


Ilustración 33. Asignación de roles de gestión

6.4 SERVIDORES DE AUTENTICACIÓN

La autenticación de inicio de sesión único (SSO) permite a las organizaciones gestionar de forma centralizada la autenticación y autorización de usuarios mediante la integración con un proveedor de identidades (IdP). Con la autenticación SSO, los usuarios pueden iniciar sesión en diferentes recursos y servicios empresariales con un único conjunto de credenciales (nombre de usuario y contraseña). Puede configurar proveedores de identidades habituales como Microsoft Entra ID (anteriormente Azure AD) y Okta, o bien optar por la autenticación multifactorial mediante la integración con Duo. Este enfoque permite a su organización controlar el acceso de los usuarios de forma eficiente y garantiza que estos puedan acceder de forma fácil y segura a los recursos necesarios.

Para la configuración del mecanismo de SSO con los distintos proveedores de identidades, dado que los mecanismos suelen cambiar, o se pueden añadir nuevos proveedores, se recomienda revisar la guía de configuración [REF2]. A fecha de redacción de la presente guía de hoy los proveedores soportados son los siguientes:

- Microsoft ADFS
- Microsoft Entra ID
- Octubre
- Inicio de sesión único
- Identidad de ping
- PingFederate
- Servidor SAML genérico
- Espacio de trabajo de Google
- Dúo
- RADIO

En la tabla inferior se muestra qué características admite Infinity Portal por cada proveedor de identidad:

Proveedor de identidad (IdP)	SAML	Flujo iniciado por el IdP	Integración de directorios - Manual	Integración de directorios - SCIM
Microsoft Entra ID	Sí	Sí	Solo para servicios de Check Point .	Solo para servicios de Check Point .
Octubre	Sí	Sí	Solo para servicios de Check Point .	Solo para servicios de Check Point .
Inicio de sesión único	Sí	Sí	Solo para servicios de Check Point .	Solo para servicios de Check Point
Identidad de ping	Sí	Sí	Solo para servicios de Check Point .	Solo para servicios de Check Point
Espacio de trabajo de Google	Sí	Sí	Solo para servicios de Check Point .	No
Microsoft ADFS	Sí	No	Solo para servicios de Check Point .	No
PingFederate	Sí	Sí	No	No
Dúo	Sí	No	No	No
Servidor SAML genérico	Sí	No	No	No

Ilustración 34. Tabla de capacidades

6.5 SINCRONIZACIÓN

El portal sincroniza automáticamente la hora con los servidores de Check Point.

6.6 ACTUALIZACIONES

Al tratarse de un servicio SaaS, las actualizaciones necesarias serán realizadas de forma transparente por el fabricante.

6.7 ALTA DISPONIBILIDAD

Al tratarse de un servicio SaaS, el mecanismo de alta disponibilidad es transparente para el usuario. No obstante, Check Point pone a disposición de sus clientes la url de monitorización de recursos [REF 6] donde se puede validar el estado de los distintos servicios incluidos Infinity Portal y los servicios asociados:

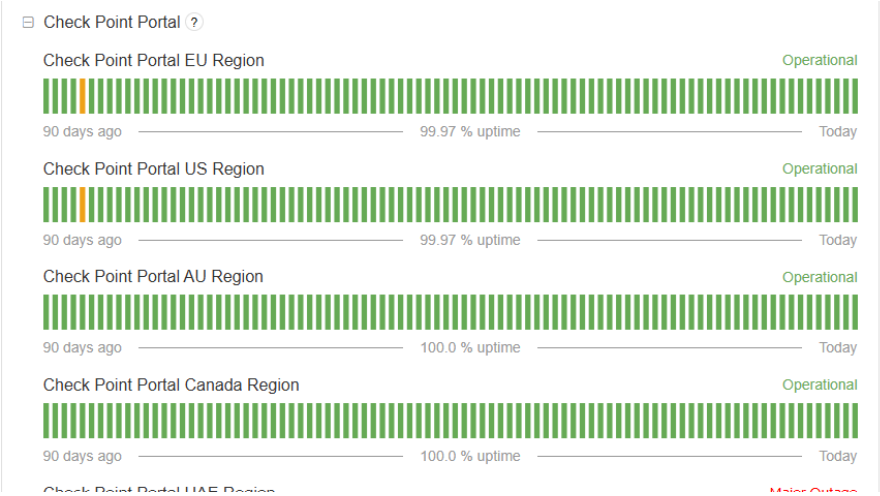


Ilustración 35. URL de monitorización de recursos

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS

Infinity Portal genera únicamente logs de auditoría. Estos logs pueden consultarse en el menú de configuración, Audits:

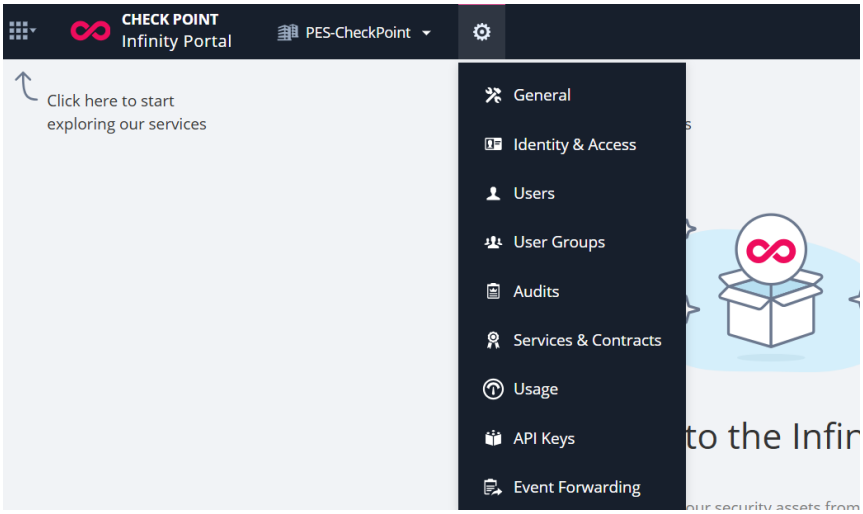


Ilustración 36. Opciones del Infinity Portal

En este apartado se muestran todos los logs referentes a cambios realizados por los administradores.

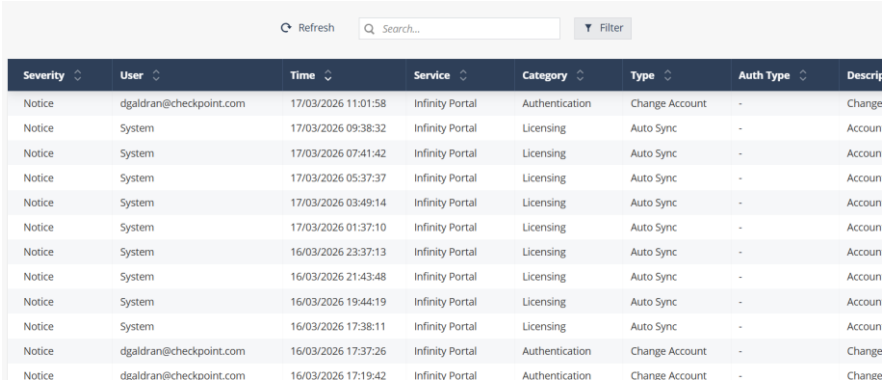


Ilustración 37. Vista de eventos del portal

6.8.2 ALMACENAMIENTO REMOTO

El reenvío de logs a un syslog no se hace desde Infinity Portal sino desde las aplicaciones que corren en ella, por ejemplo, gestión de endpoint, gestión de firewalls, etc. Por tanto debe hacerse allí la integración con SIEMs o el reenvío a servidores remotos.

6.9 BACKUP

Al tratarse de una herramienta SaaS el backup se ejecuta en la Cloud del propio prestador del servicio.

7 REFERENCIAS

REF1 Check Point Infinity Portal Admin Guide
https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/CP_Infinity_Portal_AdminGuide.pdf

REF2 Manual Infinity Portal. Sección Single Sign On
(https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Content/Topics-Infinity-Portal/Users-Settings.htm?tocpath=Account%20Settings%7CUsers%7C_____0#Adding_and_Editing_User_Accounts

REF3 Portal de clientes (licencias). (https://usercenter.checkpoint.com)

REF4 Video explicativo para la creación del portal
https://app.guidde.com/share/playbooks/odCDMy885uy24DQCwUZtHk

REF5 Url de Infinity Portal. https://portal.checkpoint.com

REF6 URL Monitorización de recursos https://status.checkpoint.com

REF7 CPSTIC
https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

REF8 Manual Infinity Portal. Sección Administradores.
https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Content/Topics-Infinity-Portal/Users-Settings.htm

REF9 Manual Infinity Portal. Sección Roles de servicio.
https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Infinity-Portal-Admin-Guide/Content/Topics-Infinity-Portal/Users-Settings.htm#User_Roles

8 ABREVIATURAS

ADFS	Active Directory Federation Services
API	Application Programming Interface
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.
CSV	Comma-Separated Values
Etc	Etcétera
ID	Identity
IdP	Identity Provider
SaaS	Software as a Service
SAML	Security Assertion markup Language
SSO	Single Sign On