Guia de instalación y uso de la herramienta para el análisis del Directorio Activo/Entra ID/Okta (PurpleKnight)

País del cliente

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

Índice

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

1. Antes de empezar

Este documento te guía, paso a paso, en la instalación y el uso del programa que analiza la seguridad de tu directorio activo de identidades corporativas dentro de tu servicio de Análisis de Vulnerabilidades. No hace falta que tengas conocimientos técnicos: si sigues los pasos en orden, en unos 15-20 minutos tendrás el informe listo para compartir con tu consultor.

El programa se llama Purple Knight y sirve para revisar la configuración de tu Directorio Activo, Microsoft Entra ID u Okta en modo de solo lectura: identifica configuraciones inseguras y posibles rutas de ataque, y genera un informe que tu consultor asignado podrá analizar después. No cambia nada en tu infraestructura ni instala software adicional en tus sistemas: solo lee y genera un archivo con el resultado.

Puedes encontrar la guía oficial de instalación, en inglés, en el siguiente enlace de github: SOFT_Purple_Knight/Purple-Knight-User-Guide (2).pdf at main · CheKecha19/SOFT_Purple_Knight

¿Es seguro instalar y ejecutar este programa?

Sí, y es un paso imprescindible para poder generar el informe de tu análisis: sin él no se puede completar esta parte del servicio. Purple Knight solo lee la configuración de tu entorno; no modifica nada ni envía información a ningún sitio distinto del informe que tú mismo guardarás en tu equipo.

Lo descargarás siempre desde la página oficial del fabricante (lo verás en el Paso 1) es posible que, al descargarlo, Windows muestre un aviso de seguridad: es un comportamiento estándar del sistema operativo con cualquier programa descargado de internet, no un indicio de que el archivo sea malicioso, y se resuelve en menos de un minuto siguiendo el Paso 2 de esta guía. Si en algún momento tienes dudas, tu consultor te acompañará en cada paso durante la reunión inicial.

1.1 Qué necesitas antes de empezar

Antes de instalar el programa, comprueba que tienes:

- Un ordenador con Windows y permisos para ejecutar programas .exe
- Conexión al entorno que vayas a analizar: Directorio Activo, Entra ID u Okta
- Credenciales de solo lectura para ese entorno (en el apartado 2.5 te explicamos cuáles y por qué son solo de lectura)

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

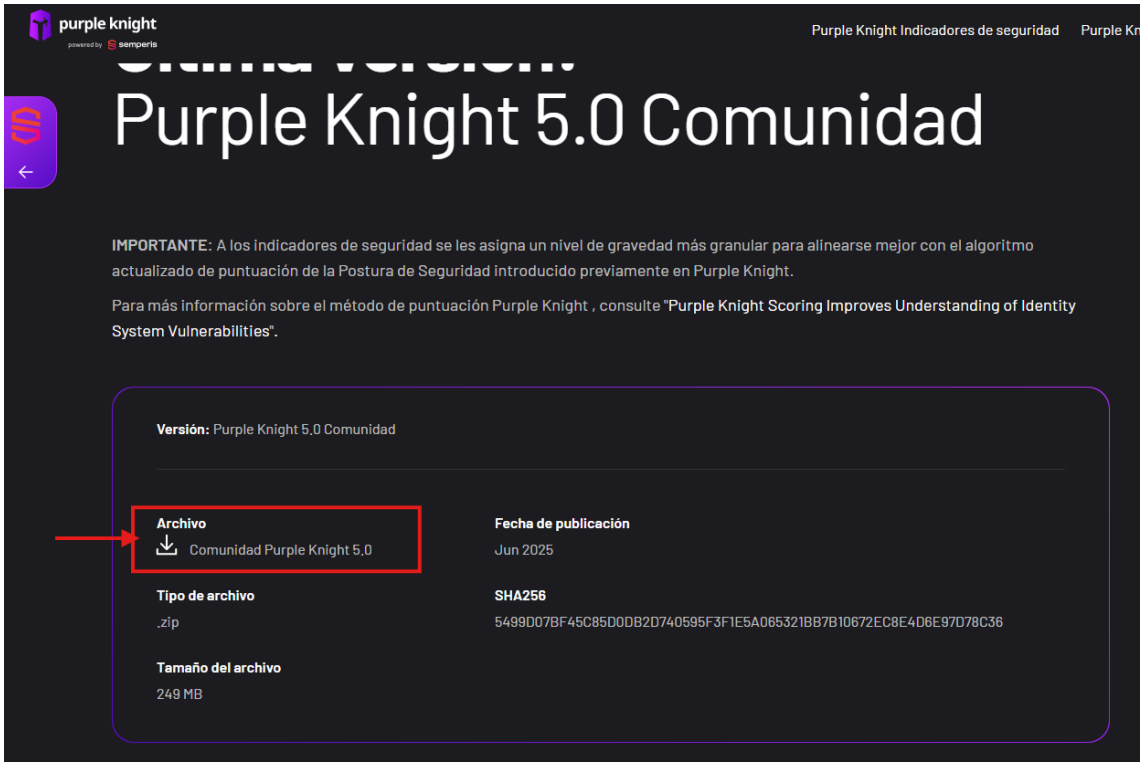
- Entre 15 y 20 minutos sin interrupciones, ya que el análisis no debe pausarse mientras se ejecuta

Si no tienes claro cuál de estos entornos usa tu empresa, o quién de tu equipo puede facilitarte las credenciales, coméntalo con tu consultor: es un tema habitual y se resuelve fácilmente en la reunión inicial.

2. Instalación y ejecución, paso a paso

2.1 Paso 1 — Descarga el programa

Accede a la página oficial de descarga: https://www.semperis.com/es/purple-knight/resources/ Es la página del fabricante de la herramienta, así que es la fuente que debes usar siempre. Busca el botón de descarga y sigue las instrucciones para obtener el archivo comprimido (ZIP).



Web de descarga Purple Knight

El archivo se descargará como un ZIP. No lo abras todavía: en el siguiente paso te explicamos cómo desbloquearlo antes de extraerlo.

2.2 Paso 2 — Desbloquea el archivo descargado

Como el archivo viene de internet, Windows puede bloquearlo por precaución. Es un aviso habitual y no significa que el programa sea malicioso; simplemente hay que decirle a Windows que confías en el origen del archivo.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

1. Haz clic derecho sobre el archivo ZIP y selecciona *Propiedades*
2. En la parte inferior de la ventana, marca la casilla *Desbloquear*
3. Pulsa *Aplicar* y después *Aceptar*

Este paso es importante: si extraes el ZIP antes de desbloquearlo, el programa puede no funcionar correctamente. Si ya lo has extraído, borra la carpeta, desbloquea el ZIP original y vuelve a extraerlo.

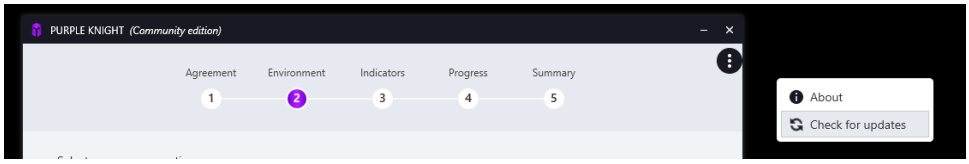
2.3 Paso 3 — Extrae y ejecuta el programa

Extrae el contenido del ZIP en una carpeta local sencilla, por ejemplo `C:\PK`. Evita carpetas sincronizadas con OneDrive o rutas de red: pueden causar errores más adelante.

Dentro de la carpeta, haz doble clic en el archivo PurpleKnight.exe para abrir el programa.

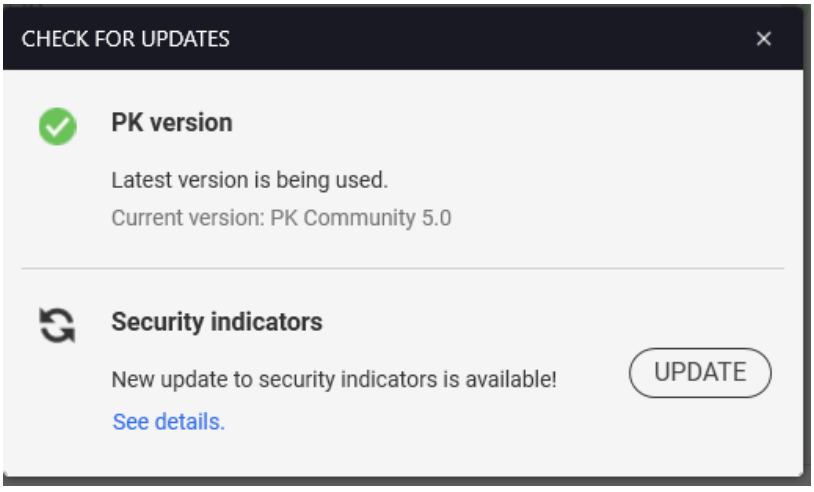
2.4 Paso 4 — Comprueba si hay actualizaciones

Al abrirse el programa, comprueba si hay una versión más reciente de los indicadores de seguridad: así te aseguras de que el análisis sea lo más completo posible. Haz clic en los tres puntos de la esquina superior derecha y selecciona “Check for updates”.



Menú superior derecho para acceder a Check for updates.

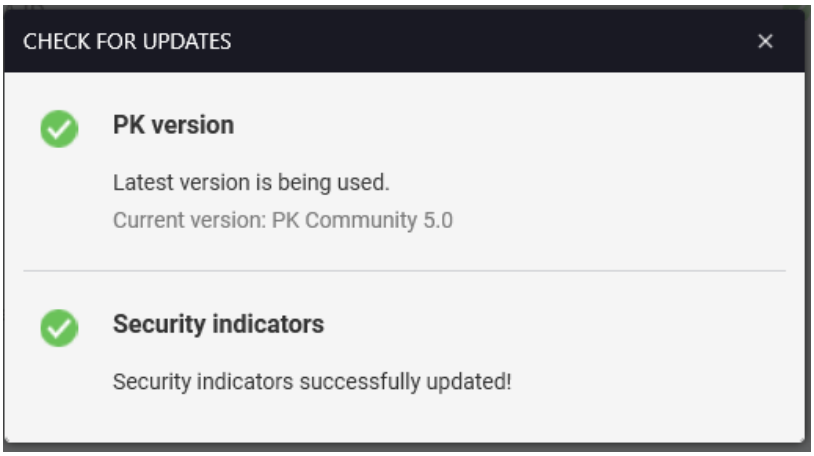
Si hay una actualización disponible, instálala antes de continuar.



***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

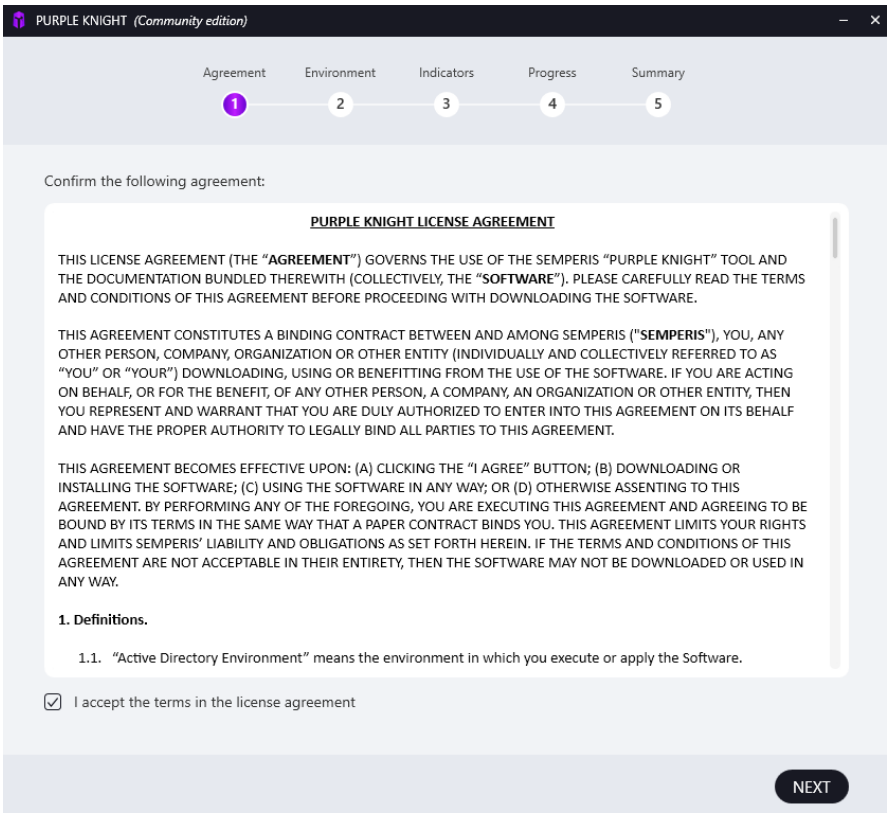
Actualización disponible de los indicadores de seguridad.



Indicadores de seguridad actualizados correctamente.

2.5 Paso 5 — Acepta el acuerdo y selecciona tu entorno

En el primer paso del asistente, revisa el acuerdo de licencia, marca la aceptación de los términos y pulsa Next.



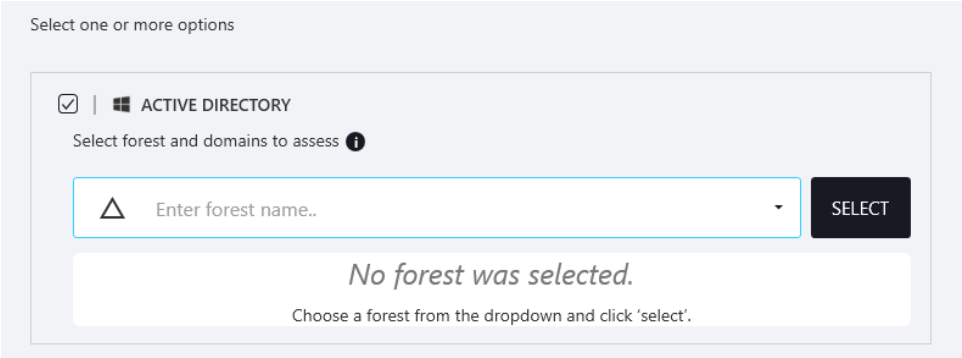
Pantalla de aceptación del acuerdo de licencia.

A continuación, selecciona el entorno que corresponde a tu empresa: Directorio Activo, Entra ID u Okta. Si conviven varios en tu organización, puedes seleccionar más de uno.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

Solución	Qué es	Dónde se usa
Active Directory	Directorio de identidades instalado en los servidores de la empresa (on-premise).	Empresas con infraestructura propia.
Microsoft Entra ID	Directorio de identidades en la nube de Microsoft.	Empresas que utilizan Microsoft 365, Azure, Teams, etc.
Okta	Plataforma independiente de gestión de identidades y acceso (IAM) en la nube.	Empresas con aplicaciones de distintos fabricantes o entornos híbridos.



Selección del entorno a analizar.

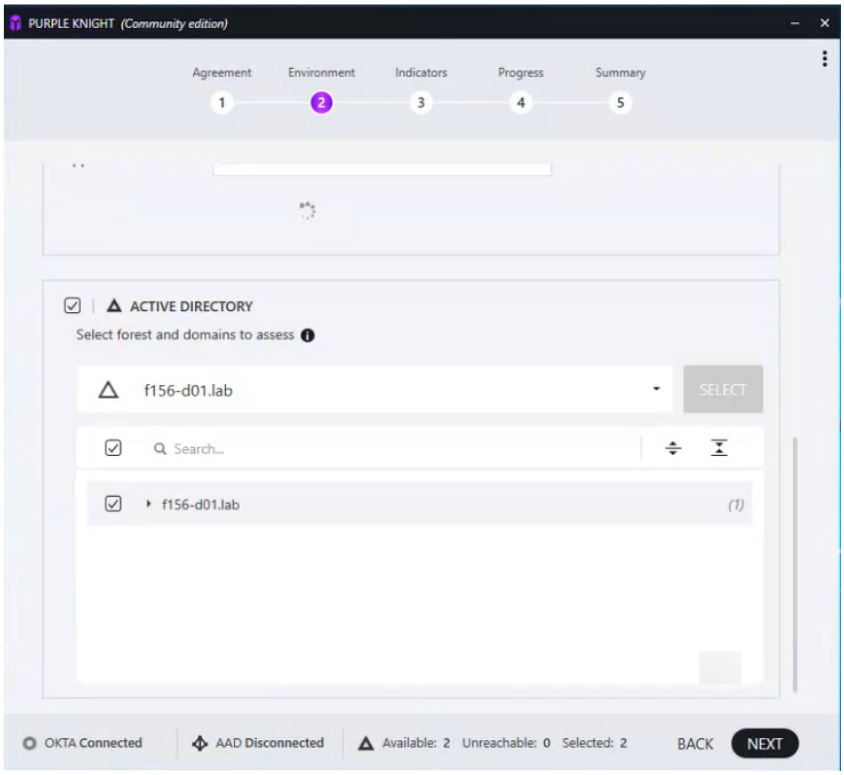
Entorno	Qué te pedirá el programa
Directorio Activo local	Un usuario de dominio con permisos de lectura, y conexión a los controladores de dominio desde el mismo equipo donde ejecutes el programa. **Más detalle en Cómo conectar con Active Directory con permisos de lectura**

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

Entra ID	Los datos de una aplicación registrada en tu organización (Tenant ID, Application ID y un secreto) con permisos de administrador. Si no la tienes creada, tu consultor te ayuda a hacerlo. Más detalle en Cómo otorgar permisos de lectura en Entra ID
Okta	El dominio de Okta de tu empresa y un token de acceso de solo lectura. Más detalle en Cómo configurar una conexión con Okta ID con permisos de lectura

Cómo conectar con Active Directory con permisos de lectura



Selección del “forest” o bosque:

Purple Knight descubre la topología y detecta el bosque actual. Por defecto, se muestra el bosque actual; si no se detecta ninguno, el campo quedará en blanco. Puede especificar un bosque de confianza introduciendo su FQDN, nombre NetBIOS o dirección IP.

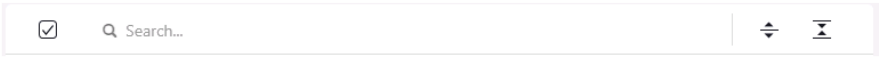
***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

Selección de dominio

Una vez validado el bosque haciendo clic en el botón SELECCIONAR, Purple Knight valida la conexión y las credenciales del usuario. Si las credenciales son insuficientes, se le pedirá que introduzca credenciales válidas (es decir, necesita permisos de lectura para consultar el bosque). Una vez validadas la conexión y las credenciales del usuario, Purple Knight devuelve una lista de los dominios disponibles.

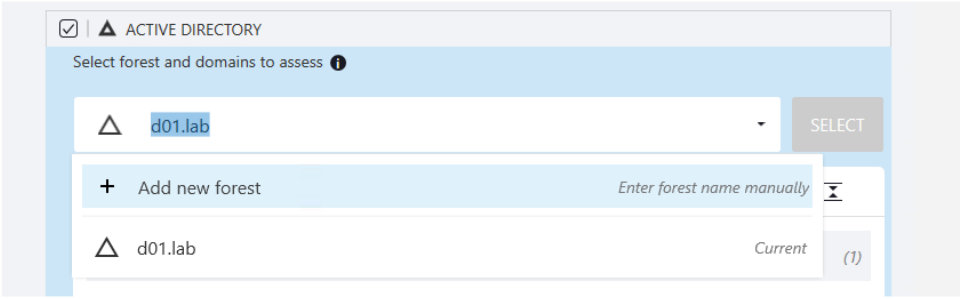
Todos los dominios disponibles están seleccionados por defecto. La fila situada encima de la lista de dominios incluye controles que permiten seleccionar o deseleccionar todos los dominios del bosque seleccionado, buscar un dominio por nombre y expandir o contraer la lista de dominios.



En el panel DIRECTORIO ACTIVO, seleccione el bosque.

• De forma predeterminada, se muestra el bosque actual.

• Para seleccionar un bosque alternativo, haga clic en la flecha desplegable, seleccione Agregar nuevo bosque e ingrese el FQDN, el nombre NetBIOS o la dirección IP del bosque.



2. Después de seleccionar un bosque, haga clic en SELECCIONAR. Al hacer clic en este botón, se iniciará una búsqueda de dominios dentro del bosque seleccionado.

3. Seleccione los dominios que desea incluir.

- Para seleccionar todos los dominios del bosque, marque la casilla "Seleccionar todo" en la fila situada encima de la lista de dominios. (Predeterminado)
- Para seleccionar dominios individuales, desmarque la casilla correspondiente a los dominios que desea excluir del informe. También

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

puede desmarcar la casilla "Seleccionar todo" y marcar la casilla a la izquierda de los dominios que desea incluir.
- Si el dominio contiene subdominios, el número de subdominios se muestra a la derecha del nombre del dominio. Haga clic en la flecha de expansión del dominio para ver los subdominios. Desmarque la casilla correspondiente a los subdominios que desea excluir o desmarque la casilla "Seleccionar todo" y marque la casilla a la izquierda de los subdominios que desea incluir.

Debajo de la lista de dominios, verá la cantidad de dominios disponibles, inaccesibles y seleccionados, así como botones para navegar a la página siguiente o anterior.

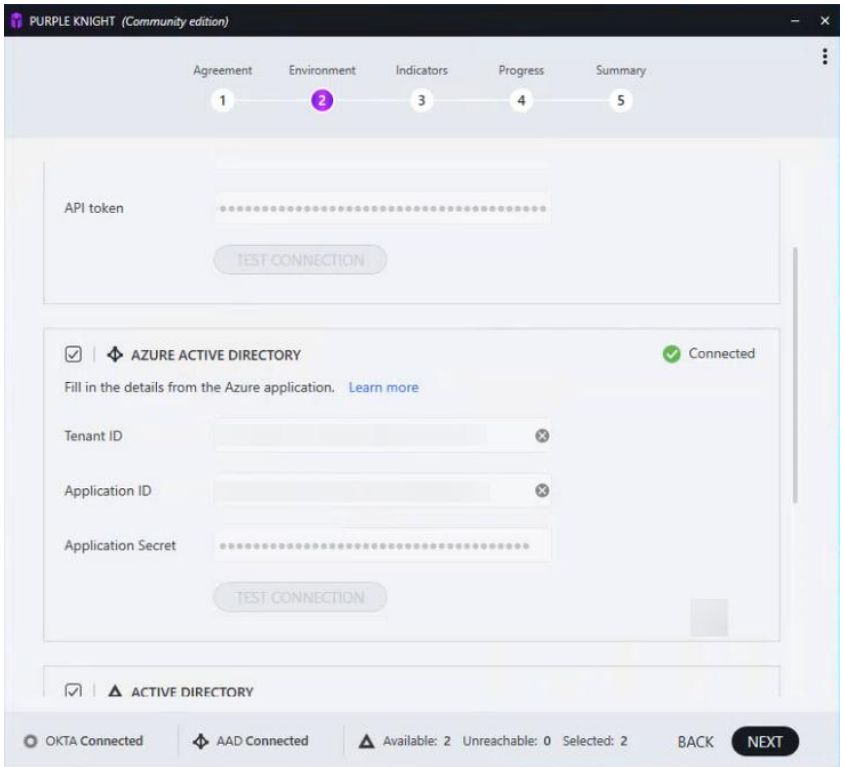
4. Si desea ver la postura de seguridad general en su entorno de identidad híbrida, seleccione los entornos correspondientes.

- Seleccione la casilla de verificación OKTA para especificar el dominio de Okta que se incluirá en la evaluación.
- Seleccione la casilla de verificación AZURE ACTIVE DIRECTORY para especificar el inquilino de Azure AD que se incluirá en la evaluación.

5. En la parte inferior de la página Entorno, asegúrese de que todos los entornos seleccionados se hayan conectado correctamente.

Cómo otorgar permisos de lectura en Entra ID

Como se aprecia en la imagen, debemos introducir los siguientes datos:



***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

Accede al panel de Azure

Para crear un registro de aplicación Purple Knight:

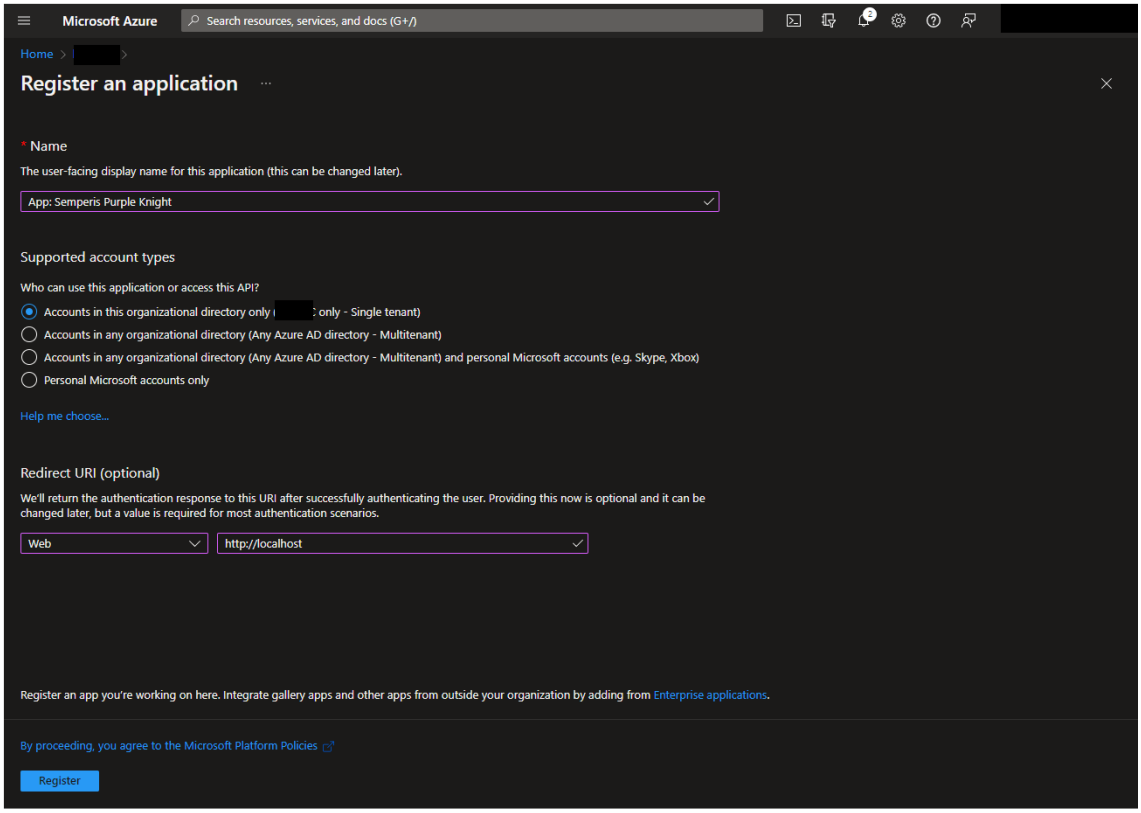
1. En el portal de Azure, seleccione el servicio Azure Active Directory.

2. En el portal de Azure AD, seleccione Registros de aplicaciones en el menú Administrar del panel de navegación.

3. Haga clic en + Nuevo registro.

4. En la pantalla Registrar una aplicación, introduzca un nombre descriptivo para su aplicación Purple Knight.

Puede usar la configuración predeterminada para las demás opciones (es decir, Tipos de cuenta admitidos: Inquilino único, URI de redireccionamiento).



5. Haga clic en el botón Registrar.

Una vez que la aplicación se registre en Azure AD, se mostrará la página de la aplicación recién registrada.

Para agregar permisos a la aplicación Purple Knight:

1. En el portal de Azure AD, seleccione la aplicación Purple Knight.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

2. Seleccione Permisos de API en el menú Administrar del panel de navegación.

La tabla Permisos configurados en la pantalla Permisos de API muestra el acceso otorgado a la aplicación. Inicialmente, verá que se le ha asignado el permiso predeterminado (User.Read).

3. Haga clic en + Agregar un permiso.

4. En el panel Permisos de API de solicitud (panel derecho), seleccione Microsoft Graph.

5. Haga clic en Permisos de la aplicación.

En el panel Seleccionar permisos, busque y seleccione los siguientes permisos de aplicación (fijarse que todos son “read all” no incluir ningún permiso de escritura por seguridad):

- AdministrativeUnit.Read.All
- Application.Read.All
- AuditLog.Read.All
- Device.Read.All
- Directory.Read.All
- Policy.Read.All
- PrivilegedAccess.Read.AzureAD
- Reports.Read.All
- RoleManagement.Read.All
- RoleManagement.Read.Directory
- User.Read.All
- UserAuthenticationMethod.Read.All

Haga clic en el botón Agregar permisos.

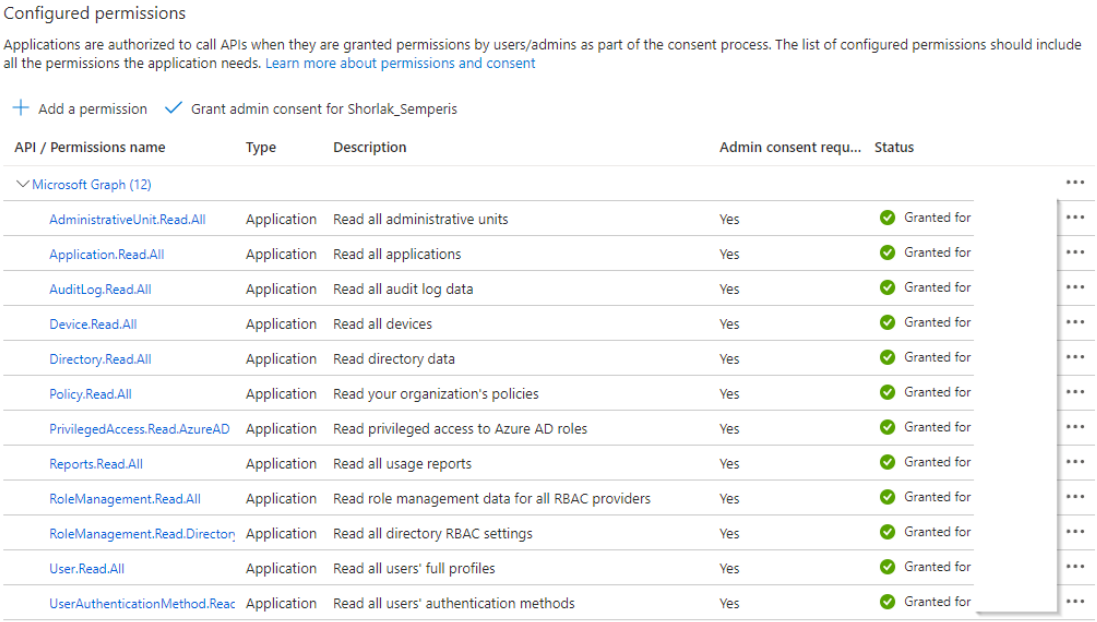
6. De vuelta en la pantalla de permisos de API, haga clic en **“Otorgar consentimiento de administrador para <tenant de Azure AD>.”**

En el mensaje de confirmación "Otorgar consentimiento de administrador" en la parte superior de la página, haga clic en Sí.

Una vez otorgados los permisos correctamente, el estado mostrará una marca de verificación verde y el mensaje **"Otorgado para <tenant de Azure AD>"** para los permisos mencionados.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.



Aviso:

1. En el portal de Azure AD, seleccione la aplicación Purple Knight y, a continuación, seleccione Información general en el menú de navegación.

- En la página Información general, copie el valor del ID de directorio (inquilino) y péguelo en el campo ID de inquilino de la página Entorno de Azure AD
- En la página Información general, copie el valor del ID de aplicación (cliente) y péguelo en el campo ID de aplicación de la página Entorno de Azure AD en Purple Knight.

2. En el portal de Azure AD, dentro de la aplicación Purple Knight, seleccione Certificados y secretos en el menú Administrar.

- En el panel Secreto de cliente, haga clic en + Nuevo secreto de cliente.
- En el panel Agregar un secreto de cliente (panel derecho), introduzca la siguiente información:
  - Descripción: Introduzca un texto descriptivo para su secreto de cliente.
  - Caducidad: Seleccione la duración del secreto de cliente.
- Haga clic en Agregar/añadir.

3. De vuelta en la pantalla Certificados y secretos, se mostrará el secreto.

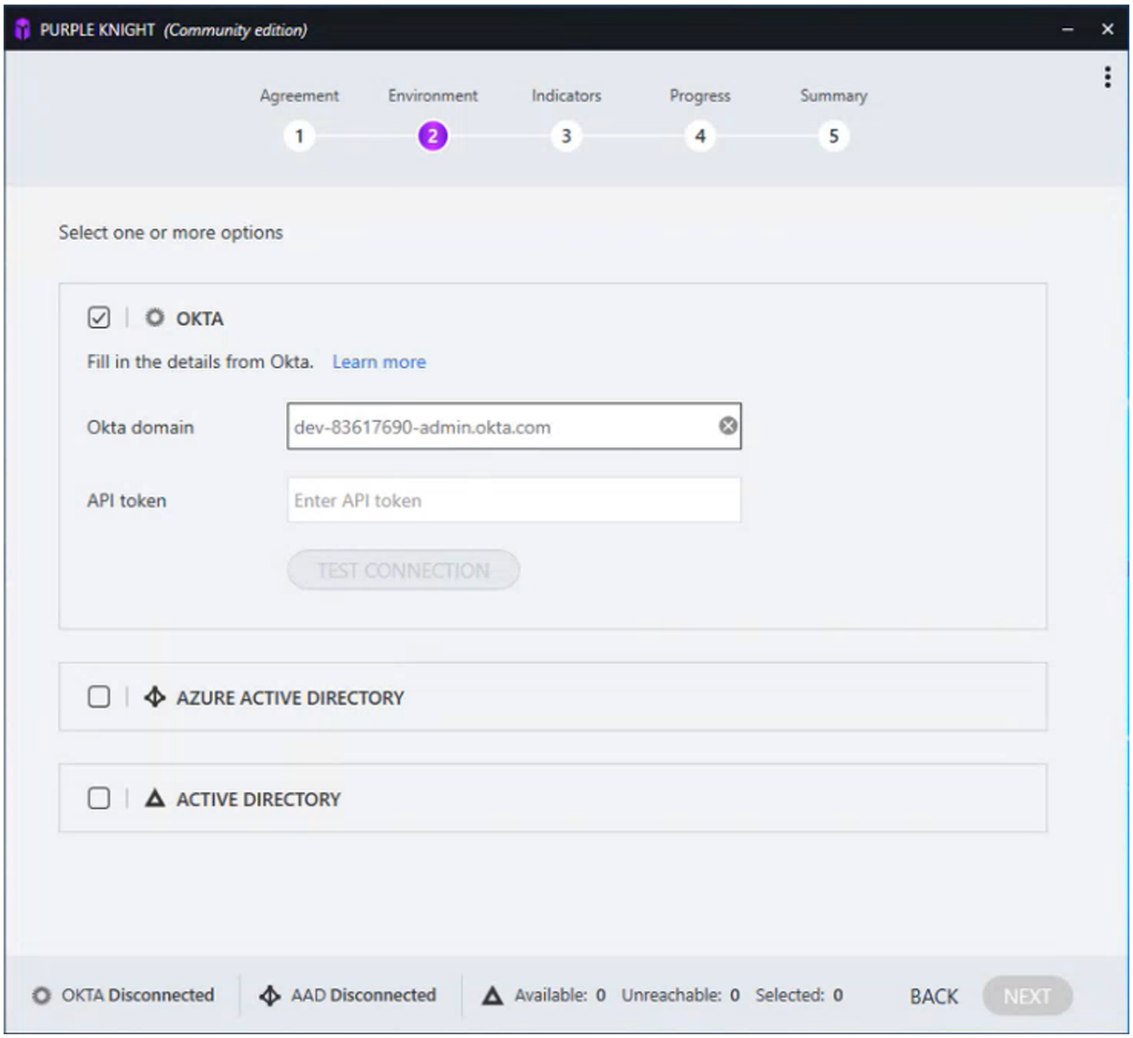
4. Copia el valor del secreto y pégalo en el campo "Secreto de la aplicación" de la página "Entorno de Azure AD" en Purple Knight. CUIDADO: No confundir “Application Secret ID” con el propio “Application Secret”. El valor que debemos

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

utilizar en Purple Knight es el segundo. El ID es solo un identificador, no un secreto.

Cómo configurar una conexión con Okta ID con permisos de lectura



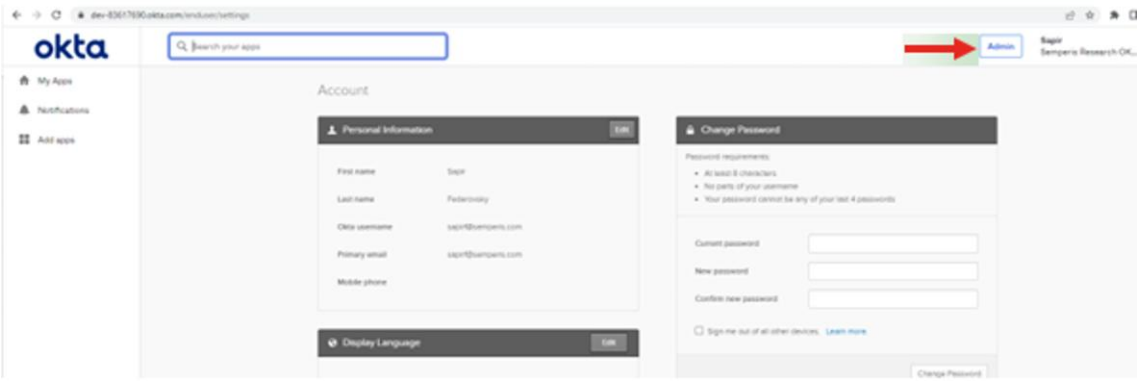
Abre la consola de administración de Okta como administrador y clica en el botón de Administrador:

Para configurar una conexión de Okta:

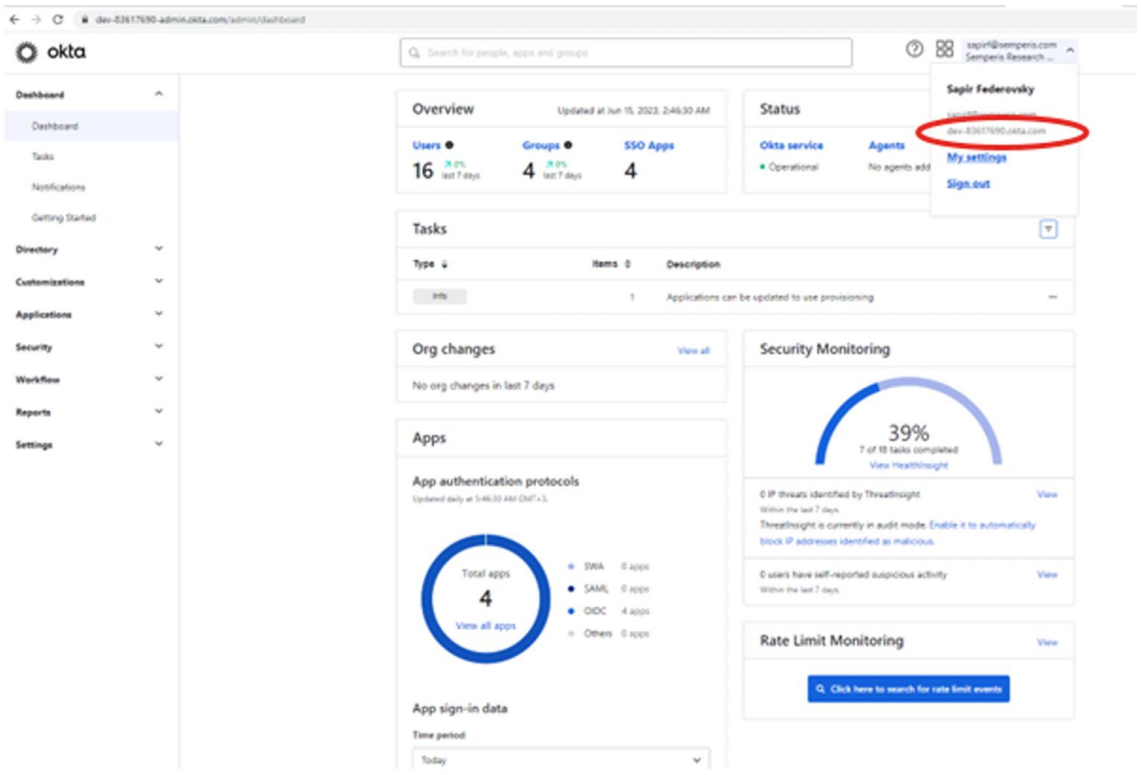
1. En la página de Entorno en Purple Knight, selecciona OKTA.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.



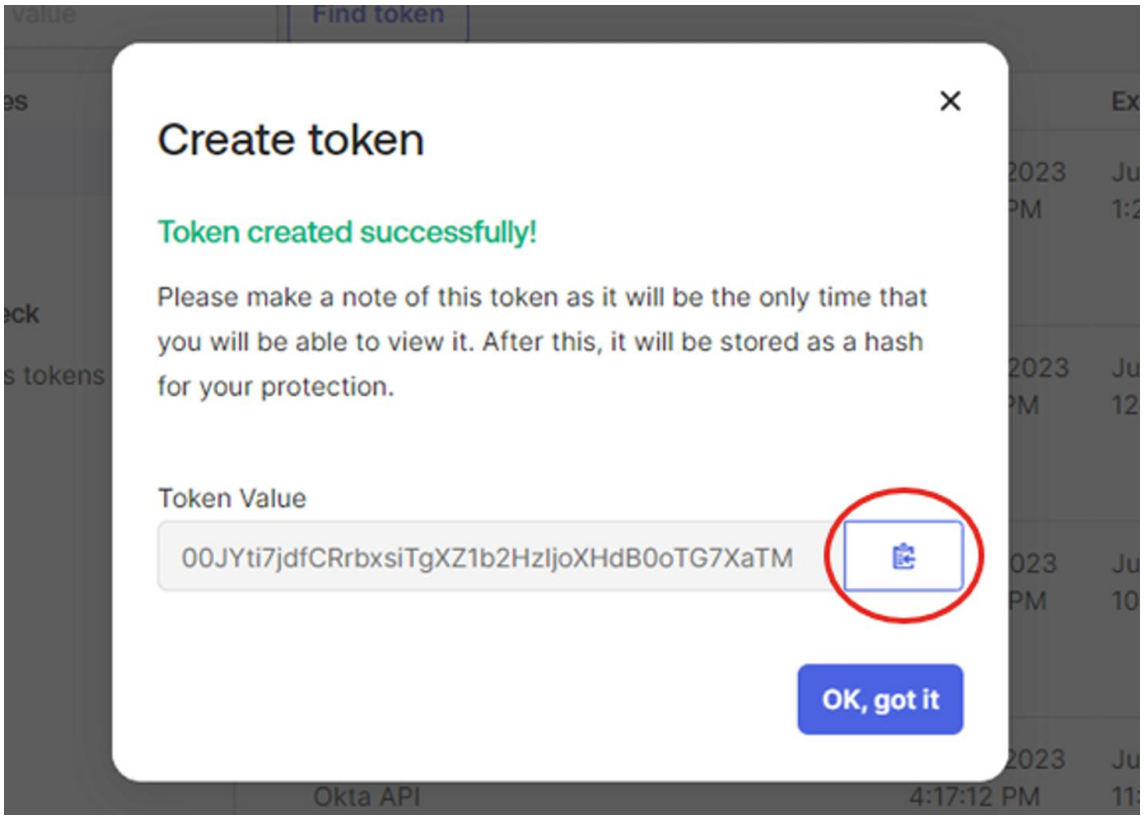
2. En el panel ampliado de OKTA, ingresa la siguiente información desde la consola de administrador de Okta:
    - Dominio de Okta: La URL del dominio de administrador, que es igual que la URL del dominio pero incluye "-admin". Por ejemplo, si la URL del dominio es: testing123.okta.com, la URL del dominio de administrador sería: testing123-admin.okta.com. (Consola de administrador de Okta: La URL del dominio se puede encontrar en las propiedades del usuario, que se pueden ver al ampliar la cuenta del usuario en la fila del encabezado)



    - Token de API: El identificador único de la aplicación que se asignará a la aplicación Purple Knight. (Consola de Admin de Okta: Para el token de API, navega a Seguridad > API > Fichas y selecciona Crear token. En el cuadro de diálogo “Token creado con éxito”, usa el botón de copiar a la derecha del campo Valor del Token para capturar el token de API. Este es el valor que Purple Knight necesita y, como dice el mensaje del cuadro, solo está disponible desde este cuadro.)

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.



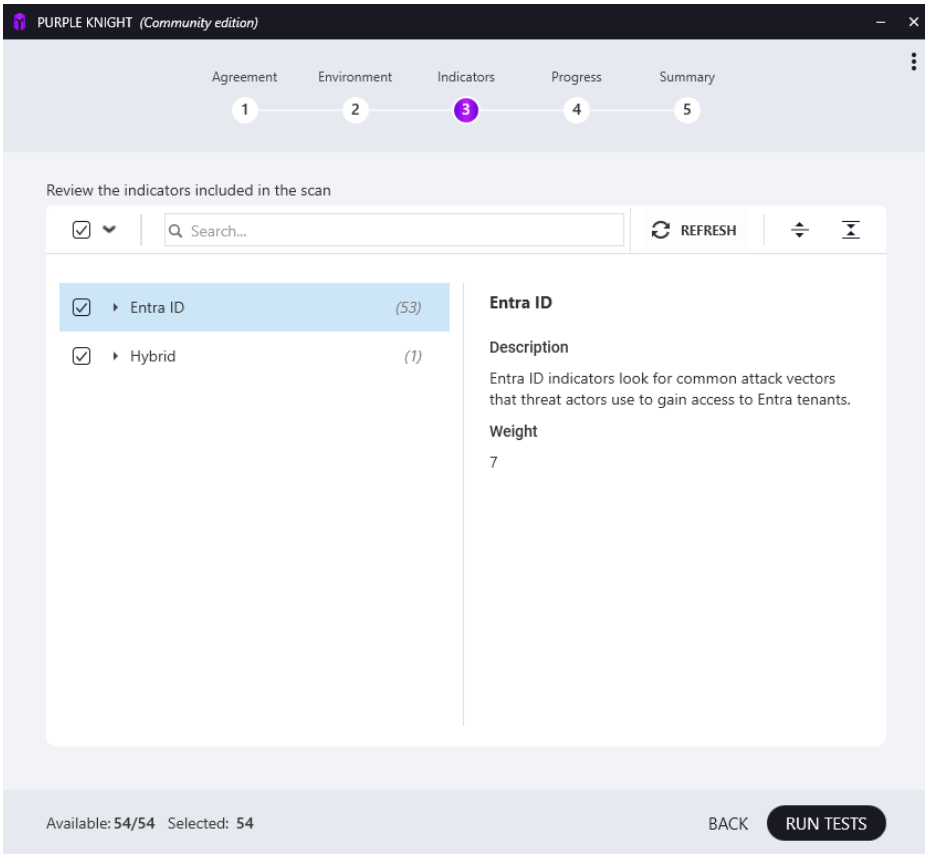
3. Tras introducir la información requerida, haz clic en PROBAR CONEXIÓN. Si la conexión fue exitosa, aparecerá un indicador de Conectado en la esquina superior derecha del panel de OKTA. Además, se muestra "OKTA Conectado" en la parte inferior de la página. (Los recuentos de dominio (Disponibles, Inaccesibles y Seleccionados) no se aplican a tu conexión de Okta.).
4. Si quieres ver la postura general de seguridad en tu entorno de identidad híbrida, selecciona los entornos adecuados.
    - Marca la casilla de ACTIVE DIRECTORY para seleccionar el “forest” y los dominios que se incluirán en la evaluación. Para más información, consulta la página de Entorno: Active Directory.
    - Marca la casilla de AZURE ACTIVE DIRECTORY para especificar el inquilino de Azure AD que se incluirá en la evaluación. Para más información, consulta la página de Entorno: Azure Active Directory.
5. Al final de la página de Entorno, asegúrate de que todos los entornos seleccionados se hayan conectado correctamente.
6. Introduce los datos de la API en el “wizard” de Purpleknight y haz clic en “Siguiente”

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

2.6 Paso 6 — Lanza el análisis

Antes de empezar, el programa te muestra los indicadores que se van a revisar. No hace falta que cambies nada: la configuración por defecto es la que necesitamos para tu análisis.

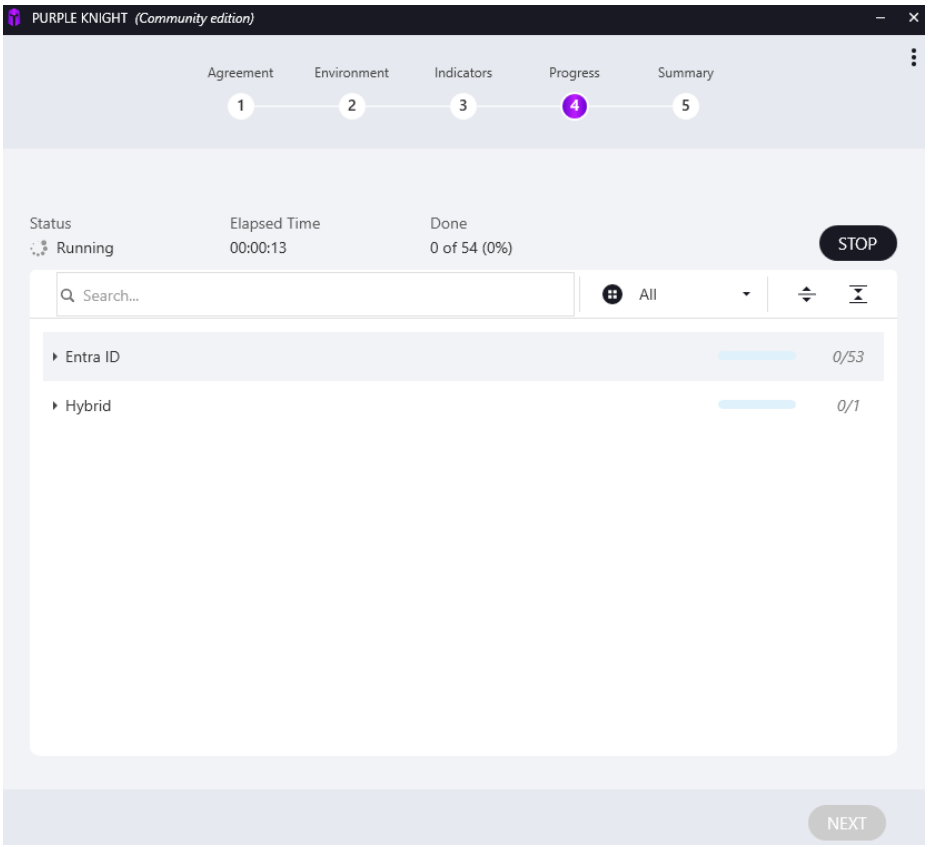


Revisión de indicadores antes de iniciar el análisis.

Pulsa Run Tests para lanzar el análisis. Mientras se ejecuta, no cierres el programa ni dejes que el ordenador se bloquee o entre en suspensión.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

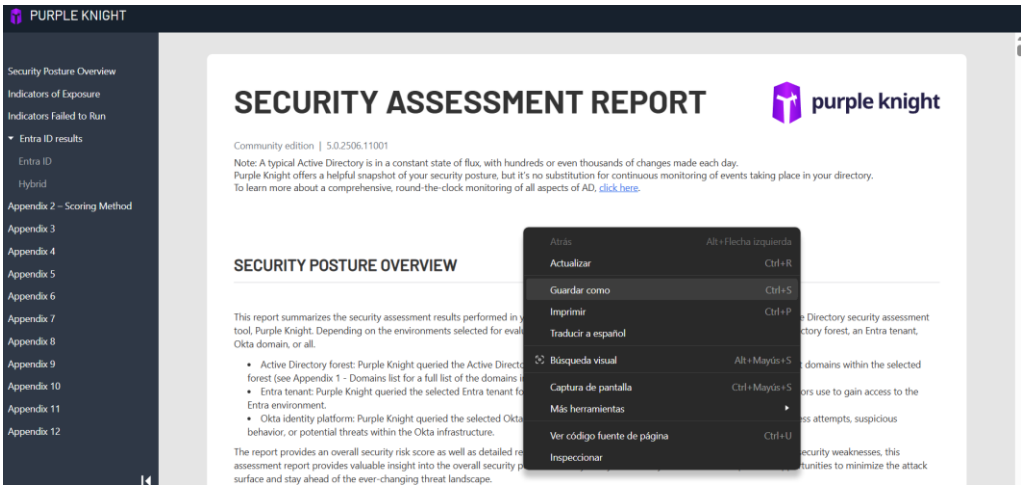
***This document is classified as PUBLIC by TELEFÓNICA.



Progreso del análisis en ejecución.

2.7 Paso 7 — Guarda el informe

Al terminar, el programa muestra un resumen de resultados y abre el informe completo en tu navegador.

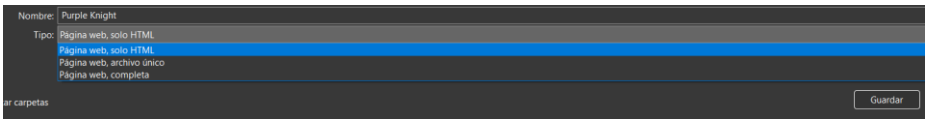


Informe de resultados abierto en el navegador.

Guarda una copia local con la opción Guardar como (Save as) de tu navegador.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.



Guardado del informe desde el navegador.

Recomendaciones para guardarlo sin problemas:

- Guarda el informe en una carpeta local sencilla, por ejemplo `C:\PK\Reports`
- Usa un nombre de archivo simple, sin caracteres especiales
- Evita guardar en OneDrive, SharePoint sincronizado o carpetas de red
- Cierra cualquier informe anterior que tengas abierto antes de generar uno nuevo

2.8 Paso 8 — Comparte el informe con tu consultor

Con el archivo del informe guardado en tu equipo, ya has terminado la parte que te corresponde. Envíaselo a tu consultor por el canal que os haya indicado durante la reunión inicial: él se encarga de analizarlo e incorporarlo al resto de tu servicio.

3. Si algo no sale como esperabas

3.1 Windows dice que el archivo está bloqueado

Vuelve al Paso 2 de esta guía y repite el proceso de desbloqueo. Si ya habías extraído el ZIP antes de desbloquearlo, borra la carpeta extraída, desbloquea el ZIP original y vuelve a extraerlo.

Si prefieres resolverlo desde la línea de comandos (o tu equipo de IT lo prefiere), este comando de PowerShell desbloquea todos los archivos de la carpeta a la vez. Sustituye la ruta por la que hayas usado tú:

```
Get-ChildItem -Path "C:\PK" -Recurse | Unblock-File
```

3.2 El análisis termina, pero no encuentras el informe

- Revisa la carpeta donde indicaste que se guardara, y también la carpeta Descargas
- Si el informe se abrió en el navegador, pero no lo guardaste, repite el Guardar como (Save as) desde la pantalla de resultados

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

- Comprueba que tu antivirus no ha bloqueado la creación del archivo
- Comprueba que la carpeta de destino no está sincronizada con OneDrive, SharePoint o una ruta de red
- Cierra cualquier informe anterior que tengas abierto antes de volver a intentarlo

Si tras revisar estos puntos sigues sin encontrar el informe, coméntaselo a tu consultor: en la mayoría de los casos basta con repetir el guardado desde la pantalla de resultados.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.

www.telefonica.com

***Este documento está clasificado como PUBLICO por TELEFÓNICA.

***This document is classified as PUBLIC by TELEFÓNICA.