



Guía del usuario de Tenable Identity Exposure SaaS

Última revisión: abril 02, 2025



Índice

Le damos la bienvenida a la Guía del usuario de Tenable Identity Exposure SaaS	11
Acerca de esta guía	11
Comenzar a usar Tenable Identity Exposure SaaS	12
Comprobar los requisitos previos	13
Instalar	13
Configurar	14
Usar	14
Expandir Tenable Identity Exposure a Tenable One	14
Requisitos anteriores a la implementación	16
Consulte también	24
Requisitos de hardware	25
Requisitos de red	25
Matriz de flujos de red	27
Requisitos de Secure Relay	39
Requisitos del portal web	46
Integración en un dominio de Active Directory	47
Secure Relay de Tenable Identity Exposure	48
Requisitos de Secure Relay	57
Configurar Relay	63
Instalar Secure Relay (CLI)	65
Instalar Secure Relay (Agente de Tenable Nessus)	66
Solucionar problemas de instalación de Secure Relay	68
Comenzar a usar Tenable Identity Exposure	77



Aspectos esenciales de Tenable Identity Exposure	103
Iniciar sesión en Tenable Identity Exposure	103
Portal del usuario de Tenable Identity Exposure	108
Acceder a “Espacio de trabajo”	112
Preferencias del usuario	115
Notificaciones	118
Tableros de control	120
Widgets	124
Centro de exposición	128
Requisitos previos	129
Consulte también	130
Información general sobre la exposición	130
Información del encabezado	131
Lista de debilidades	131
Opciones de búsqueda, filtrado, exportación y visualización de columnas	132
Consulte también	137
Instancias de exposición	137
Información general	138
Información detallada	138
Analizar los hallazgos	140
Detalles de los hallazgos	142
Opciones de búsqueda, filtrado y exportación	145
Para filtrar la lista de debilidades:	146
Consulte también	147



Identidad 360: gestión integral de riesgos de identidad	147
Recopilación de identidades	150
Inquilino, dominio y organización del IdP	150
Datos entre productos (orígenes de datos)	151
Elementos principales	154
Consulte también	155
Detalles de identidad	155
Para acceder a esta página:	155
Encabezado y sección superior	156
Pestañas de encabezado	158
	165
Aspectos esenciales de Identidad 360	169
Para aplicar un filtro:	170
Para exportar datos:	172
Para personalizar la visualización de las columnas:	173
Columnas predeterminadas	174
Para restablecer las columnas predeterminadas:	175
Descripción de la pertenencia a inquilinos	175
Vincular activos a un inquilino	175
Identificar al inquilino	175
Ejemplo	175
Casos especiales: descripción de los vínculos de los dominios raíz de bosques	176
Qué son los dominios raíz de bosques	176
Cómo surgen los casos especiales	176



Ejemplo	176
Ejemplo	177
Por qué es importante	177
Por qué eligió Tenable Identity Explorer “inquilino” como nombre del contenedor raíz	177
Trail Flow	178
Tabla “Trail Flow”	180
Buscar en Trail Flow con el asistente	182
Buscar en Trail Flow de forma manual	184
Personalizar las consultas de Trail Flow	185
Marcar consultas	188
Historial de consultas	191
Mostrar eventos anómalos	192
Detalles del evento	194
Cambios de atributos	197
Casos de uso de Trail Flow	200
Indicadores de exposición	204
Fecha de detección y resolución de anomalías	206
Detalles del indicador de exposición	207
Objetos anómalos	210
Buscar objetos anómalos	212
Ignorar un objeto anómalo o un motivo (anomalía)	216
Atributos incriminatorios	220
Indicadores de exposición basados en RSoP	222
Mejoras	223



Beneficios	224
Aspectos técnicos	224
Corregir las anomalías de los indicadores de exposición	224
Atributo adminCount definido en usuarios estándar	225
Delegación peligrosa de Kerberos.	228
Asegurar la coherencia de SDProp.	233
Indicadores de ataque	237
Detalles de un indicador de ataque	240
Incidentes de indicadores de ataque	242
Topología	248
Relaciones de confianza	249
Relaciones de confianza peligrosas	252
Ruta de ataque	253
Relaciones de ataque	259
Agregar credencial de clave	260
Agregar miembro	261
Puede actuar	263
Puede delegar	266
Pertenece a GPO	269
DCSync	270
Concesión dada para actuar	272
Tiene historial de SID	275
Toma de control implícita	277
Heredar GPO	278



GPO vinculado	280
Miembro de	282
Es propietario	283
Restablecer la contraseña	285
Gestión de RODC	287
Escribir DACL	289
Escribir propietario	291
Identificar activos de nivel 0	292
Cuentas con rutas de ataque	294
Tipos de nodos de ruta de ataque	296
Registros de actividad	299
Definiciones de entidades privilegiadas	301
Active Directory	301
Entra ID	302
Configuración y administración de Tenable Identity Exposure	303
Configuración de Active Directory	303
Acceder a objetos o contenedores de AD	303
Acceso a Análisis con privilegios	305
Implementación de indicadores de ataque	311
Instalar indicadores de ataque	314
Script de instalación de indicadores de ataque	323
Cambios técnicos e impacto potencial	332
Escenarios de ataque (< v. 3.36)	334
Instalar Microsoft Sysmon	338



Desinstalar indicadores de ataque	343
Eliminación manual de carpetas de GPO obsoletas de SYSVOL	344
Indicadores de ataque desactivados	345
Íconos de estado de la primera fila	346
Íconos de estado de las otras filas	346
Solucionar problemas de indicadores de ataque	348
Detección de antivirus	348
Prioridad de Configuración de directiva de auditoría avanzada	350
Validación del cliente de escucha de registros de eventos	352
Archivos de registros de Tenable Identity Exposure	353
Mitigación de problemas de replicación de DFS	360
Retención de registros de eventos de Windows	362
Entradas “desconocidas” en las alertas de indicadores de ataque	363
Indicadores de ataque operativos	367
Autenticación	368
Autenticación mediante Tenable One	369
Autenticación mediante una cuenta de Tenable Identity Exposure	369
Autenticación mediante LDAP	374
Autenticación mediante SAML	379
Cuentas de usuario	383
Perfiles de seguridad	386
Personalizar un indicador	388
Ajustar la personalización de un indicador	390
Roles de usuario	391



Gestionar roles	392
Establecer permisos para un rol	393
Establecer permisos en entidades de la interfaz de usuario (ejemplo)	397
Bosques	399
Gestionar los bosques	399
Proteger cuentas de servicio	400
Dominios	402
Forzar la actualización de datos en un dominio	405
Cuentas honey	406
Autenticación de Kerberos	409
Alertas	417
Configuración de servidores SMTP	417
Diferencias en la arquitectura de implementación	418
Configuración del servidor SMTP para entornos de Secure Relay	418
Configuración del servidor SMTP para entornos de VPN	419
Alertas de correo electrónico	420
Alertas de SYSLOG	424
Detalles de alertas de SYSLOG y de correo electrónico	428
Marcos de mensajes de SYSLOG	432
Verificaciones de estado	434
Lista de verificaciones de estado	439
Centro de informes	443
Compatibilidad con Microsoft Entra ID	446
Recopilación de datos de Tenable Cloud	455



Análisis con privilegios	456
Registros de actividad	457
API pública de Tenable Identity Exposure	460
Gestión de datos	462
Regiones de implementación	462
Otorgamiento de licencias de Tenable Identity Exposure	463
Gestionar la licencia	466
Prevención de errores de coincidencia de UUID de contenedores	467
Soporte a largo plazo (LTS) frente a versiones normales: diferencias y ventajas clave	470
¿Qué es LTS?	471
¿Qué son las versiones normales?	471
Diferencias clave entre las versiones LTS y normales:	471
¿Por qué elegir LTS?	471
¿Por qué elegir las versiones normales?	472
Solucionar problemas de Tenable Identity Exposure	472
Registros para solucionar problemas	472
Herramienta de diagnóstico de Tenable Identity Exposure	474
Interferencia de endurecimiento de SYSVOL con Tenable Identity Exposure	476



Le damos la bienvenida a la Guía del usuario de Tenable Identity Exposure SaaS

Última actualización: abril 02, 2025

Tenable Identity Exposure le permite prever amenazas, detectar filtraciones de datos y responder ante incidentes y ataques para proteger su infraestructura. Desde un tablero de control intuitivo que le permite supervisar su instancia de Active Directory en tiempo real, puede detectar a simple vista las vulnerabilidades más críticas, así como los procedimientos recomendados para su corrección. Los indicadores de ataque e indicadores de exposición de Tenable Identity Exposure le permiten detectar problemas subyacentes que afectan a su instancia de Active Directory, detectar relaciones de confianza peligrosas y analizar en profundidad los detalles de los ataques.

Para empezar, consulte [Comenzar a usar Tenable Identity Exposure](#).

Acerca de esta guía

En esta Guía del usuario de Tenable Identity Exposure SaaS, encontrará la siguiente información:

- La instalación de una instancia de Secure Relay.
- Las tareas que se deben hacer antes de habilitar la supervisión de seguridad.
- La configuración y el uso de Tenable Identity Exposure.

La disponibilidad de las características Indicadores de ataque e Indicadores de exposición varía en función de la licencia que haya adquirido.

Nota: Tenable Identity Exposure está disponible de manera independiente o como parte del paquete de Tenable One. Para obtener más información, consulte [Tenable One](#).

Sugerencia: La *Guía del usuario* de Tenable Identity Exposure está disponible en [inglés](#), [francés](#), [alemán](#), [japonés](#), [coreano](#), [chino simplificado](#), [español](#) y [chino tradicional](#). La interfaz de usuario de Tenable Identity Exposure está disponible en inglés, francés, alemán, japonés, coreano, chino simplificado, español y chino tradicional. Para cambiar el idioma de la interfaz de usuario, consulte [Preferencias del usuario](#).

Para obtener información adicional sobre Tenable Identity Exposure, revise los siguientes materiales de capacitación para clientes:



- [Tenable Identity Exposure Self Help Guide \(Guía de autoayuda de Tenable Identity Exposure\)](#)
- [Tenable Identity Exposure Introduction \(Tenable University\) \(Introducción a Tenable Identity Exposure \[Tenable University\]\)](#)

Plataforma de gestión de exposición Tenable One

Tenable One es una plataforma de gestión de exposición que permite a las organizaciones obtener visibilidad sobre la superficie de ataque moderna, centrar los esfuerzos en prevenir los posibles ataques y comunicar de manera precisa el riesgo cibernético para lograr un rendimiento empresarial óptimo.

La plataforma combina la cobertura de vulnerabilidades más amplia, que abarca activos de TI, recursos en la nube, contenedores, aplicaciones web y sistemas de identidad. Además, cuenta con la velocidad y la amplitud de la cobertura de vulnerabilidades de Tenable Research y agrega análisis exhaustivos para priorizar las acciones y comunicar el riesgo cibernético. Gracias a Tenable One, las organizaciones consiguen lo siguiente:

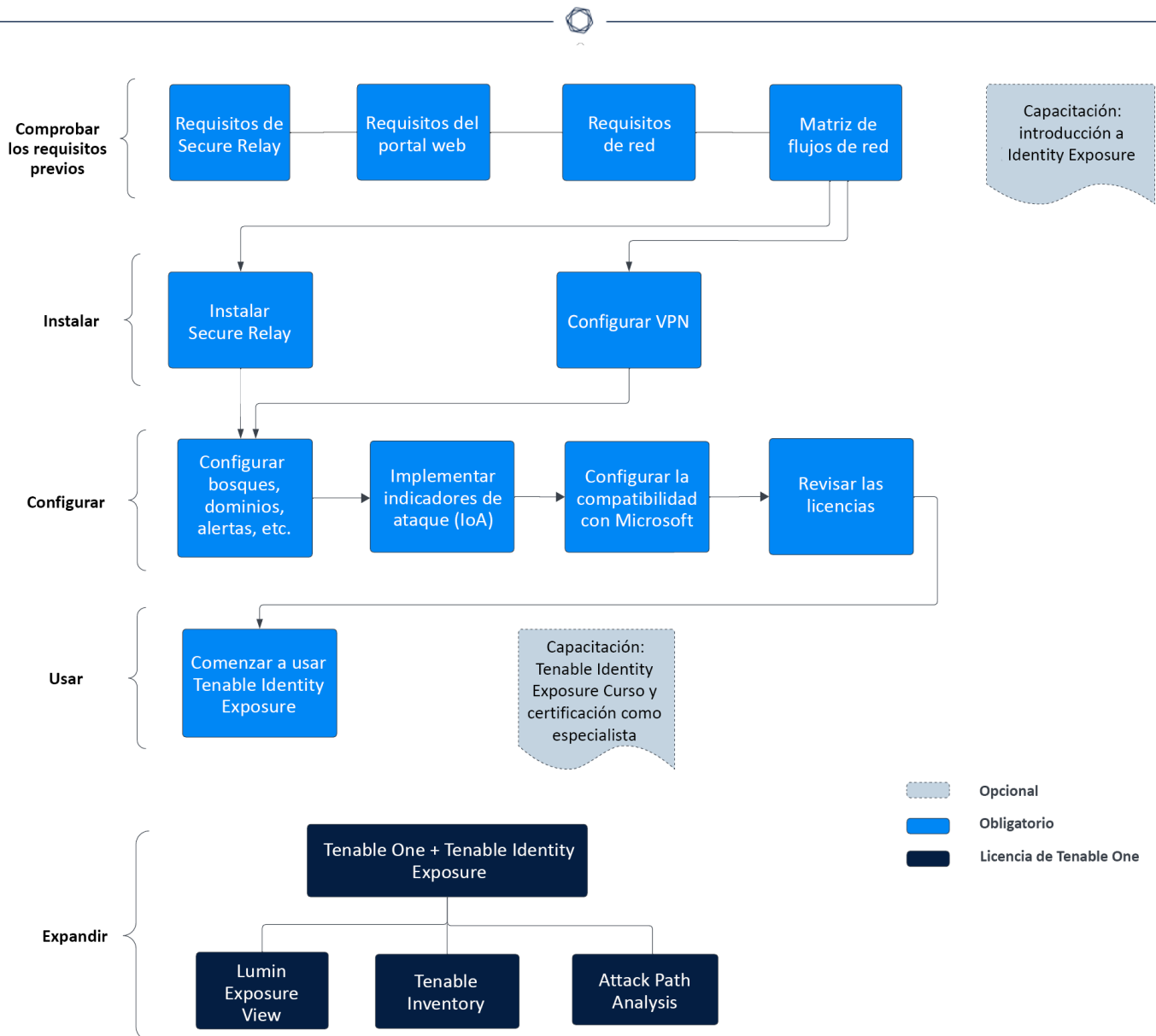
- Obtener una visibilidad completa sobre la superficie de ataque moderna.
- Prever las amenazas y priorizar los esfuerzos para evitar los ataques.
- Comunicar el riesgo cibernético para tomar mejores decisiones.

Tenable Identity Exposure existe como producto independiente o puede adquirirse como parte de la plataforma de gestión de exposición Tenable One.

Sugerencia: Para obtener información adicional sobre cómo comenzar a usar los productos de Tenable One, consulte [Tenable One Deployment Guide](#) (Guía de implementación de Tenable One).

Comenzar a usar Tenable Identity Exposure SaaS

Utilice el siguiente flujo de trabajo para implementar Tenable Identity Exposure.



Comprobar los requisitos previos

1. **Revise** las [notas de la versión](#).
2. **Revise y comprenda el rol de Secure Relay** en la plataforma Tenable Identity Exposure: a partir de la versión **3.59**, la funcionalidad obligatoria de Secure Relay le permite configurar dominios desde los cuales Relay reenvía los datos al componente de Directory Listener a cargo de recopilar los objetos de AD. Consulte [Requisitos de Secure Relay](#).

Instalar



1. **Instale** [Secure Relay de Tenable Identity Exposure](#) .

Configurar

1. **Revise** [Otorgamiento de licencias de Tenable Identity Exposure](#).

Usar

- [Comenzar a usar Tenable Identity Exposure](#)

Expandir Tenable Identity Exposure a Tenable One

Nota: Para esto se requiere una licencia de Tenable One. Si quiere obtener más información para probar Tenable One, consulte [Tenable One](#).

Integre OT Security en Tenable One y aproveche las siguientes funcionalidades:

- En [Lumin Exposure View](#), obtenga un contexto empresarial crítico mediante un valor de Cyber Exposure Score alineado con la empresa para servicios, procesos y funciones empresariales críticos, y haga un seguimiento de la entrega en relación con los SLA. Haga un seguimiento del riesgo general de las identidades para comprender la contribución en términos de riesgo de las aplicaciones web al valor general de Cyber Exposure Score.
 - Revise la [tarjeta de exposiciones Global](#) para comprender su puntuación integral. Haga clic en **Por exposición** para comprender qué factores influyen en la puntuación y en qué medida.
 - Revise la [tarjeta de exposiciones](#) de **Active Directory**.
 - [Configure las opciones de Exposure View \(Vista de la exposición\)](#) para establecer un **objetivo de tarjeta** personalizado y configurar el **SLA de corrección** y la **eficiencia del SLA** según la política de su empresa.
 - [Cree una tarjeta de exposiciones personalizada](#) según el contexto empresarial (por ejemplo, dominios, administradores de dominio, criticidad de los activos, usuarios/activos críticos o cuentas de servicio).



- En [Tenable Inventory](#), acceda a información más detallada sobre los activos —incluidas rutas de ataque relacionadas, etiquetas, tarjetas de exposiciones, usuarios, relaciones y más —para mejorar la inteligencia de estos. Para mejorar la puntuación del riesgo, obtenga una visión más completa de la exposición de los activos, con un valor de Asset Exposure Score que evalúa el total de riesgo de los activos y de criticidad de los activos para las identidades.
 - Revise los activos de AD para comprender la naturaleza estratégica de la interfaz. Esto debería ayudarlo a establecer sus expectativas sobre qué funcionalidades utilizar en Tenable Inventory y cuándo hacerlo.
 - Revise las [consultas de Tenable](#) que puede usar, editar y marcar como favoritas.
 - Familiarícese con el [generador de consultas de búsqueda global](#) y sus objetos y propiedades. Marque las consultas personalizadas como favoritas para usarlas más adelante.

Consejo: Para obtener una vista rápida de las propiedades disponibles:

- En el generador de consultas, escriba *has*. Aparece una lista de propiedades de activos sugeridas.
- Agregue una columna para personalizar la lista. Aparece una lista de columnas o propiedades disponibles.

- Explore la página [Detalles del activo](#) para ver las propiedades del activo y todas las vistas de contexto asociadas.
 - (Opcional) [Cree una etiqueta](#) que combine distintas clases de activos.
- En [Attack Path Analysis](#), optimice la priorización de riesgos al exponer rutas de ataque de riesgo que atraviesen la superficie de ataque —incluidas aplicaciones web, TI, OT, IoT, identidades o ASM —y evite un impacto sustancial. Para optimizar la mitigación, detecte los puntos críticos para interrumpir las rutas de ataque con orientación de mitigación y obtenga una amplia experiencia con información de IA.
 - Consulte el [tablero de control Attack Path Analysis \(Análisis de ruta de ataque\)](#) para obtener una vista general de sus activos vulnerables, como la cantidad de rutas de ataque que conducen a estos activos críticos, la cantidad de hallazgos abiertos y su gravedad, una matriz para ver rutas con diferentes combinaciones de puntuación de exposición del nodo de origen y valor objetivo de ACR, y una lista de tendencias de rutas



de ataque.

- Revise la **matriz de rutas de ataque principales** y haga clic en el mosaico **Rutas de ataque principales** para ver más información sobre las rutas que conducen a sus “joyas de la corona” o administradores de dominio.

Puede ajustar estas opciones si es necesario para asegurarse de estar viendo los datos y hallazgos de la ruta de ataque más críticos.

- En la página [Hallazgos](#), vea todas las técnicas de ataque que existen en una o más rutas de ataque que conducen a uno o más activos críticos; para ello, combine sus datos con análisis de gráficos avanzados y el marco MITRE ATT&CK® para crear hallazgos, que le permiten comprender las incógnitas que hacen posible y amplifican el impacto de las amenazas en sus activos e información y actuar en consecuencia.
- En la página [Detección](#), genere consultas de rutas de ataque para ver sus activos como parte de posibles rutas de ataque:
 - [Generar una ruta de ataque mediante una consulta integrada](#)
 - [Generar una consulta de activos mediante el generador de consultas de activos](#)
 - [Generar una consulta de rutas de ataque mediante el generador de consultas de rutas de ataque](#)

Luego, puede ver los datos de [Consulta de rutas de ataque](#) y [Consulta de activos](#) e interactuar con ellos a través de la lista de resultados de la consulta y el [gráfico interactivo](#).

Requisitos anteriores a la implementación

Antes de comenzar, compruebe que se cumplen los siguientes requisitos previos para garantizar un proceso de instalación fluido.

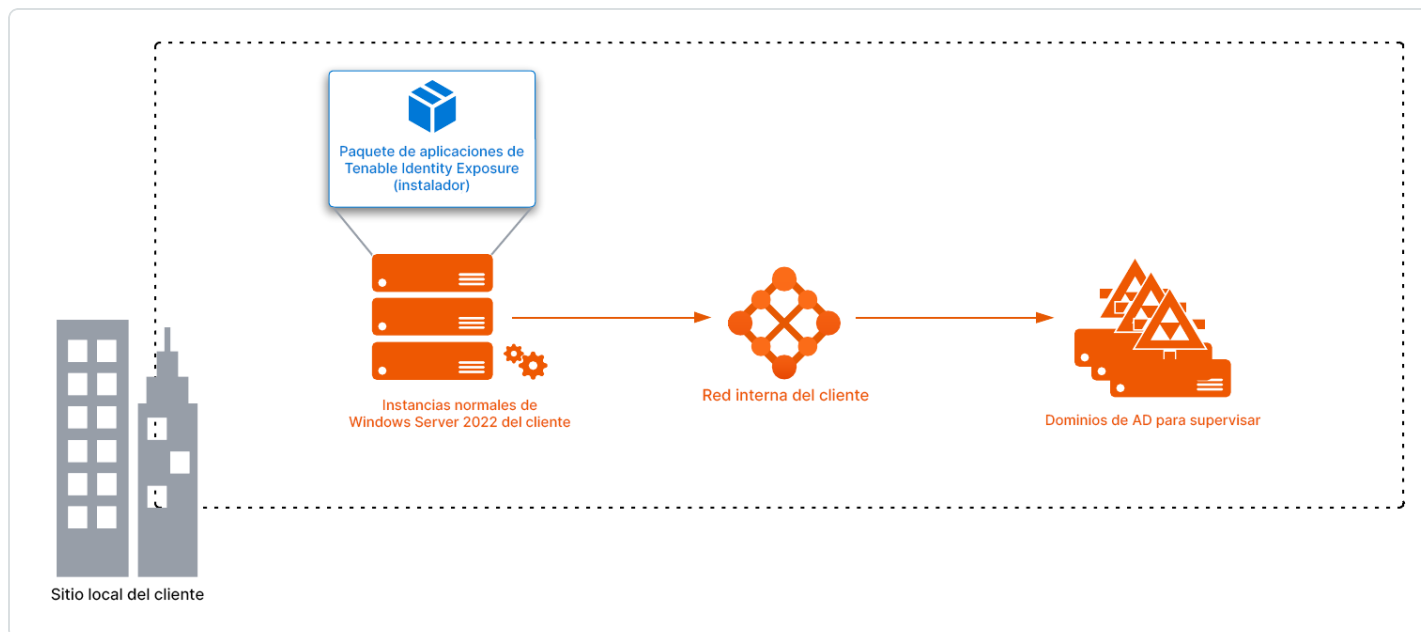
Información general de la instalación

Tenable Identity Exposure se instala como paquete de aplicaciones alojado en un entorno de Windows dedicado que debe cumplir especificaciones de alojamiento específicas. Tenable Identity Exposure requiere acceso a la imagen maestra del sistema operativo en el sistema donde se instala.



Tenable preconfigura el paquete de aplicaciones solo con los servicios de Tenable y sus requisitos específicos. Esta opción de implementación ofrece la máxima flexibilidad y se integra a la perfección en el entorno específico.

Tenable Identity Exposure se ejecuta en una arquitectura de microservicios incrustada en los servicios de Windows. Estos servicios tienen un propósito específico (almacenamiento, análisis de seguridad, aplicación, etc.) y son todos obligatorios. Por lo tanto, solo puede instalar Tenable Identity Exposure en sistemas operativos que admitan el modelo de microservicios.



Certificados TLS

Compatibilidad con OpenSSL 3.0: a partir de la versión **3.59.5**, Tenable Identity Exposure utiliza **OpenSSL 3.0.x**. Como consecuencia, los certificados X.509 firmados con SHA1 ya no funcionan en el nivel de seguridad 1 o superior. El nivel de seguridad predeterminado de TLS es el 1, lo que hace que los certificados firmados con SHA1 no sean de confianza para autenticar servidores o clientes.

Tiene que actualizar los certificados en respuesta a este cambio. Si continúa con la instalación sin actualizar los certificados para usar OpenSSL 3.0, el instalador de Tenable Identity Exposure devolverá los siguientes mensajes de error con las correcciones recomendadas:



Tenable Identity Exposure Setup



Error: The encryption algorithm used in the Server PFX Archive is not supported.

Solution: Please regenerate the PFX file using the supported and secure encryption algorithm OpenSSL 3.0 .

[See raw logs](#)

Raw Logs

MAC: sha1, Iteration 2048

MAC length: 20, salt length: 8

PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048

Error outputting keys and certificates

84150000:error:0308010C:digital envelope

routines:inner_evp_generic_fetch:unsupported:.. \crypto\evp\evp_fetch.c:355:

default library context, Algorithm (RC2-40-CBC : 0), Properties ()

Error: The Server PFX Archive format is invalid or the file is corrupted.

Solution: Please regenerate the PFX file using the original certificates and keys.

[See raw logs](#)

Raw Logs



Error: The provided Server PFX Archive is not valid.

Solution: Please ensure the PFX file is correct or regenerate it using the original certificates and keys.

See raw logs

Raw Logs

Privilegios de cuenta

Realice la instalación como miembro de la cuenta local del grupo de administradores local o integrado o como administrador en el servidor donde se instala Tenable Identity Exposure.

Precaución: Inicie sesión en la máquina con esta **cuenta de administrador local fuera del dominio. No inicie sesión como administrador local en el dominio.**

La cuenta requiere los siguientes permisos:

- SeBackupPrivilege
- SeDebugPrivilege
- SeSecurityPrivilege

Antivirus (AV) y detección y respuesta de puntos de conexión (EDR)

Antes de la instalación, deshabilite las soluciones de AV y EDR en el host. Si no las deshabilita, se activará una reversión durante la instalación. Puede habilitar la solución de AV o EDR de forma segura una vez que se complete la instalación, pero tenga en cuenta que puede afectar al rendimiento del producto debido al elevado número de operaciones de E/S del disco.

Reinicios pendientes

Realice todos los reinicios necesarios antes de la instalación. Cuando se inicia el instalador en un servidor, se comprueba lo siguiente:



- No hay ningún reinicio pendiente.
- El servidor se reinició correctamente hace menos de 11 minutos.
- MSI comprueba las siguientes claves de registro:
 - HKLM: \ Software \ Microsoft \ Windows \ CurrentVersion \ Component Based Servicing \ RebootPending
 - HKLM: \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ WindowsUpdate \ Auto Update \ RebootRequired
 - HKLM: \ SYSTEM \ CurrentControlSet \ Control \ Session Manager -> PendingFileRenameOperations

Cuentas de servicio

El uso de cuentas de servicio debe estar permitido en el sistema operativo.

Indicadores de ataque

El registro de eventos de Windows debe tener un tiempo de retención mínimo de 5 minutos para garantizar que la aplicación pueda recuperar con precisión todos los eventos.

Configuraciones no admitidas

En la siguiente tabla se detallan las configuraciones no admitidas:

Configuración	Descripción
Solución activa de antivirus (AV) o de detección y respuesta de puntos de conexión (EDR)	La plataforma Tenable Identity Exposure requiere un uso intensivo de E/S de disco. <ul style="list-style-type: none">• El uso de soluciones de AV y EDR puede disminuir drásticamente el rendimiento de la plataforma.• Debe tener una excepción para permitir los servicios de Tenable Identity Exposure y la carpeta de datos.
Firewalls	Haga lo siguiente para permitir que los servicios de Tenable Identity Exposure se comuniquen entre sí y puedan



	<p>supervisar la seguridad de manera confiable:</p> <ul style="list-style-type: none">• Deshabilite las reglas del firewall local que impidan el tráfico saliente.• Defina reglas del firewall local para permitir el tráfico entrante en los servicios de Tenable Identity Exposure.
Erlang	<ul style="list-style-type: none">• No personalice la variable de entorno HOMEDRIVE.• La variable de entorno PATHEXT debe contener las extensiones de archivo .exe y .bat.

Aplicaciones de terceros

Implementar la plataforma de Tenable Identity Exposure en un entorno sin certificar puede generar efectos secundarios inesperados.

En particular, la implementación de aplicaciones de terceros (como un agente o demonio en particular) en la imagen maestra puede provocar problemas de estabilidad o rendimiento.

Tenable recomienda encarecidamente reducir al mínimo la cantidad de aplicaciones de terceros.

Derechos de acceso

La plataforma de Tenable Identity Exposure requiere derechos administrativos locales para funcionar y garantizar una adecuada gestión del servicio.

- Debe proporcionar al responsable técnico de Tenable las credenciales (nombre de usuario y contraseña) asociadas a la cuenta administrativa de la máquina host.
- Cuando se implemente en un entorno de producción, considere la posibilidad de poner en práctica un proceso de renovación de contraseñas que valide junto con el responsable técnico de Tenable.

Actualizaciones del producto

Como parte del programa de actualización, Tenable publica con frecuencia actualizaciones de sus sistemas para brindar nuevas funcionalidades de detección y nuevas características de productos.



- En esta implementación, Tenable solo ofrece actualizaciones para los componentes de Tenable Identity Exposure. Debe garantizar una gestión adecuada de los sistemas operativos, incluida la implementación frecuente de parches de seguridad. Para obtener más información sobre las versiones de Tenable Identity Exposure, consulte [Notas de la versión de Tenable Identity Exposure](#).
- La arquitectura de microservicios de Tenable Identity Exposure admite la aplicación inmediata de parches del sistema operativo.

Otros requisitos

- Tenable Identity Exposure funciona con las versiones de Windows Server que se enumeran en [Requisitos de hardware](#) con la actualización más reciente que está disponible.
- El programa de instalación de Tenable Identity Exposure requiere **derechos de administrador local en Windows Server 2016 o versiones posteriores**. Si la cuenta usada para la instalación es la predeterminada, asegúrese de que esta cuenta pueda ejecutar programas sin restricciones.
- Los servicios de Tenable Identity Exposure requieren derechos de administrador local para ejecutar servicios locales en la máquina.
- Tenable Identity Exposure necesita una partición de datos dedicada. Para evitar que el sistema se congele si la partición está llena, no ejecute Tenable Identity Exposure en la partición del sistema operativo.
- La instancia de SQL de Tenable Identity Exposure requiere la funcionalidad de uso de cuentas virtuales.
- Al instalar o actualizar Microsoft SQL Server después de implementar medidas de seguridad más estrictas, el proceso de instalación falla debido a derechos de usuario insuficientes. Compruebe que tenga los permisos necesarios para una instalación correcta. Para obtener más información, consulte la [documentación de Microsoft](#).
- Tenable Identity Exposure debe funcionar como caja negra. Dedique cada máquina a Tenable Identity Exposure y no las comparta con otro producto.
- Tenable Identity Exposure puede crear cualquier carpeta que comience por el prefijo "Alsid" o "Tenable" en la partición de datos. Por lo tanto, no cree carpetas que comiencen por "Alsid" ni



“Tenable” en la partición de datos.

- Erlang: no modifique la variable de entorno HOMEDRIVE. La variable de entorno PATHEXT debe contener las extensiones de archivo .exe y .bat.
- Si tiene que definir la cuenta de servicio de AD de Tenable Identity Exposure como miembro del grupo “Usuarios protegidos”, asegúrese de que la configuración de Tenable Identity Exposure admita la [autenticación de Kerberos](#), ya que “Usuarios protegidos” no puede usar la autenticación de NTLM.

Lista de verificación previa a la instalación

En esta tabla se resumen los requisitos previos en forma de una práctica lista de verificación anterior a la instalación.

Información o recurso para reservar	Estado
Los acuerdos necesarios (acuerdos de confidencialidad, licencias de software de evaluación), si corresponde.	
La cantidad de usuarios de AD activos en los dominios objetivo que se van a supervisar.	
Los recursos de proceso y memoria se basan en la matriz de dimensionamiento de Tenable Identity Exposure. Consulte Resource Sizing.	
La IP privada de cada máquina virtual usada para implementar la plataforma de Tenable.	
El tipo y la dirección IP de la infraestructura de administración de actualizaciones, el servidor horario, el servidor de la PKI y el proveedor de identidad.	
Abra los flujos de red necesarios para cada servicio que Tenable Identity Exposure requiera. Consulte Matriz de flujos de red .	
Las direcciones IP privadas de cada emulador del controlador de dominio principal.	
Creación de una cuenta de usuario normal en cada bosque de Active Directory	



que se va a supervisar.	
En los contenedores específicos de Active Directory, otorgue derecho de acceso a la cuenta de servicio de Tenable.	
Otorgue acceso a Análisis con privilegios si quiere habilitar esta funcionalidad.	
Nombre de usuario de la cuenta de usuario del dominio de AD: <ul style="list-style-type: none">• Formato: nombre principal de usuario, por ejemplo, "tenablead@dominio.ejemplo.com" (se recomienda para la compatibilidad con Kerberos); o NetBIOS, por ejemplo, "NombreDominioNetBIOS\NombreCuentaSam".	
Un certificado TLS emitido para el portal web de Tenable Identity Exposure desde la PKI del cliente: <ul style="list-style-type: none">• De lo contrario, informe a Tenable sobre el uso del certificado autofirmado.	
La lista de cuentas de usuario de Tenable Identity Exposure que se van a crear: <ul style="list-style-type: none">• Información obligatoria: nombre y apellido, dirección de correo electrónico y nombre de usuario deseado.	
La lista de configuraciones opcionales que se van a activar (notificación por correo electrónico, reenvío de eventos de SYSLOG, etc.).	
Un coordinador de proyecto identificado y disponible para que trabaje con Tenable.	
Personal técnico para responder a posibles problemas técnicos, como problemas de filtrado de red y PDCe inaccesible.	

Consulte también

- Resource Sizing
- [Requisitos de hardware](#)
- [Requisitos de red](#)



- [Requisitos del portal web](#)
- [Integración en un dominio de Active Directory](#)

Requisitos de hardware

Tenable Identity Exposure requiere el siguiente hardware:

- Sistemas operativos Microsoft Windows compatibles
 - Windows Server 2016
 - Windows Server 2019
 - Windows Server 2022
 - Windows Server 2025
- Los requisitos descritos en las secciones de dimensionamiento son para el bienestar de la plataforma de Tenable Identity Exposure; no incluyen los requisitos del sistema operativo de una implementación basada en paquetes de aplicaciones.
- La velocidad de la CPU debe ser de al menos 2,6 GHz.
- La plataforma de Tenable Identity Exposure admite la arquitectura de procesadores x86-64 (al menos Sandy Bridge o Piledriver) con Tecnología Intel Turbo Boost 2.0.
- Una interfaz de red obligatoria: puede agregar otras interfaces de red con fines de administración, supervisión o cualquier otro motivo.

Requisitos de red

Tenable Identity Exposure requiere acceso a las infraestructuras de Active Directory para iniciar la supervisión de seguridad. Debe permitir los flujos de red entre los distintos servicios de Tenable Identity Exposure, como se describe en [Matriz de flujos de red](#).

Ancho de banda

Como plataforma de supervisión, Tenable Identity Exposure recibe eventos de Active Directory de forma continua. Según la escala de la infraestructura, este proceso puede generar un volumen significativo de datos.



Debe asignar un ancho de banda adecuado para garantizar la transmisión de datos a Tenable Identity Exposure para su análisis en un plazo razonable.

En la siguiente tabla se define el ancho de banda necesario en función del tamaño de la instancia de AD supervisada.

Usuarios de AD activos	Cantidad promedio de objetos recibidos (por minuto)	Ancho de banda mínimo	Ancho de banda recomendado
1 - 5000	10	1 Mbps	2 Mbps
5001 - 75 000	150	5 Mbps	10 Mbps
75 001 - 400 000	700	15 Mbps	30 Mbps

API de Microsoft

Para suscribirse a los flujos de replicación y comenzar a supervisarlos, Tenable Identity Exposure debe comunicarse con las API de directorio estándar de Microsoft. Tenable Identity Exposure solo requiere comunicación con el emulador del controlador de dominio principal (PDCe) con una cuenta de usuario normal. También debe implementar un nuevo objeto de política de grupo (GPO) para activar el motor de detección de ataques.

Comunicación con AD

Para una instalación local, Tenable Identity Exposure es un paquete de software que se implementa en el entorno de Windows Server. Tenable Identity Exposure debe comunicarse con la instancia de Active Directory supervisada.

Acceso a Internet

Tenable ofrece un proceso de integración continua para permitir lanzamientos habituales de nuevas funcionalidades y características de detección. Tenable recomienda que planifique un acceso a Internet para actualizar Tenable Identity Exposure periódicamente.

Protocolos de red

Protocolos de red específicos (como SYSLOG, SMTP o HTTP) permiten a Tenable Identity Exposure ofrecer funcionalidades de alerta nativas, la capacidad de diseñar flujos de análisis específicos



vinculados a una plataforma de administración de eventos e información de seguridad (SIEM) y una API de REST que puede integrarse en un ecosistema de ciberseguridad.

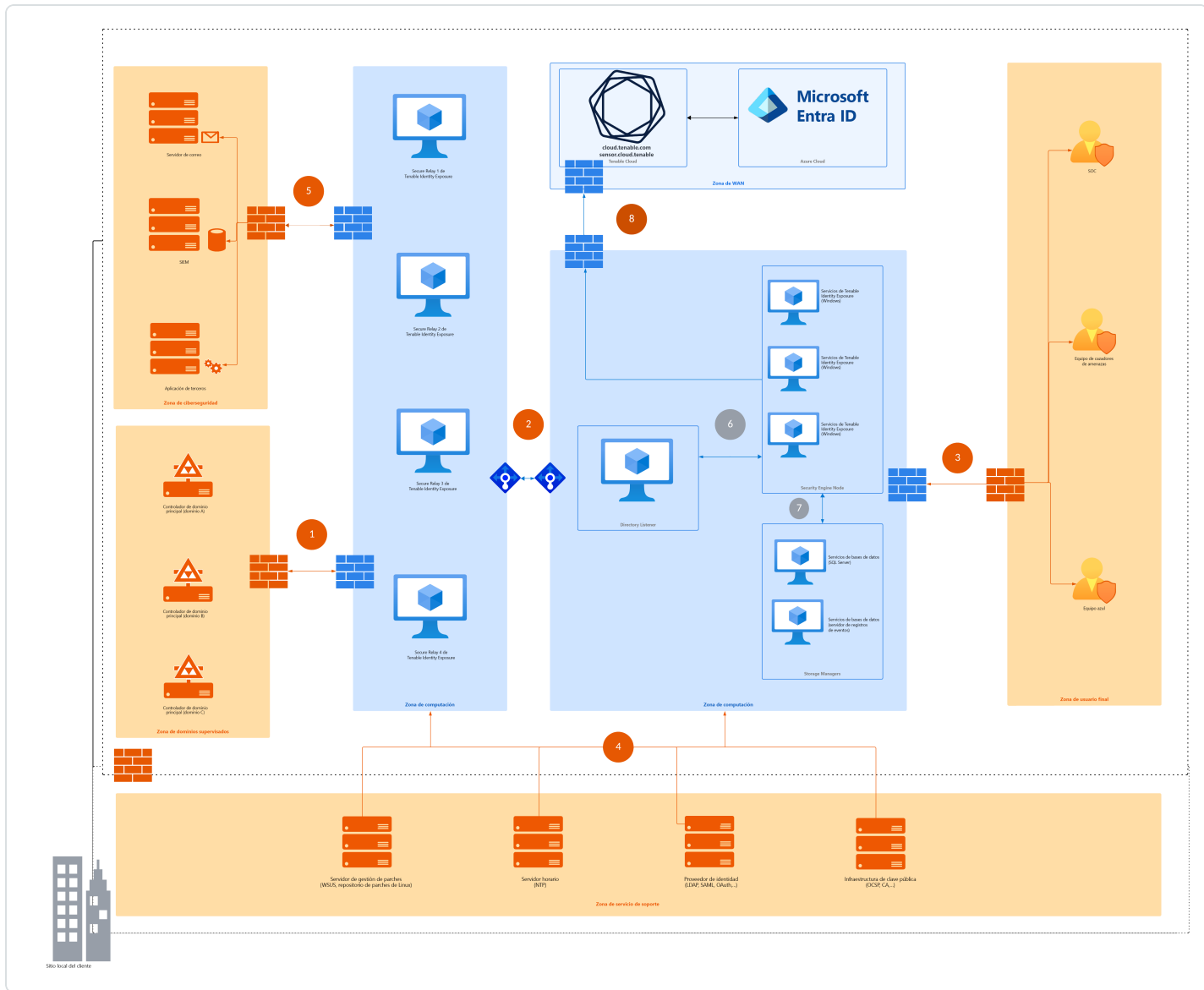
Matriz de flujos de red

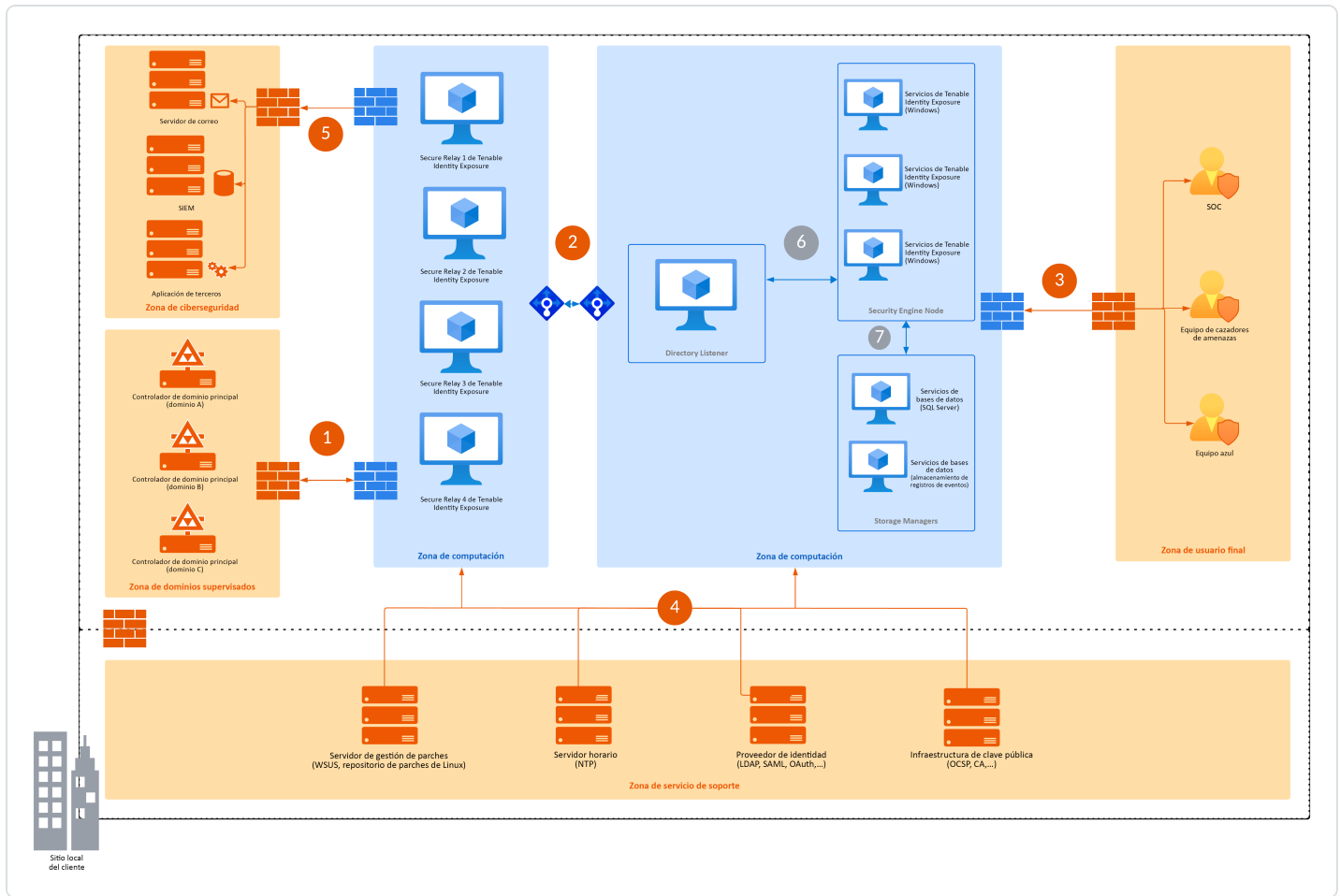
Para encargarse de la supervisión de seguridad, Tenable Identity Exposure tiene que comunicarse con el emulador del controlador de dominio principal (PDCe) de cada dominio. Debe abrir puertos de red y protocolos de transporte en cada PDCe para garantizar una supervisión eficiente.

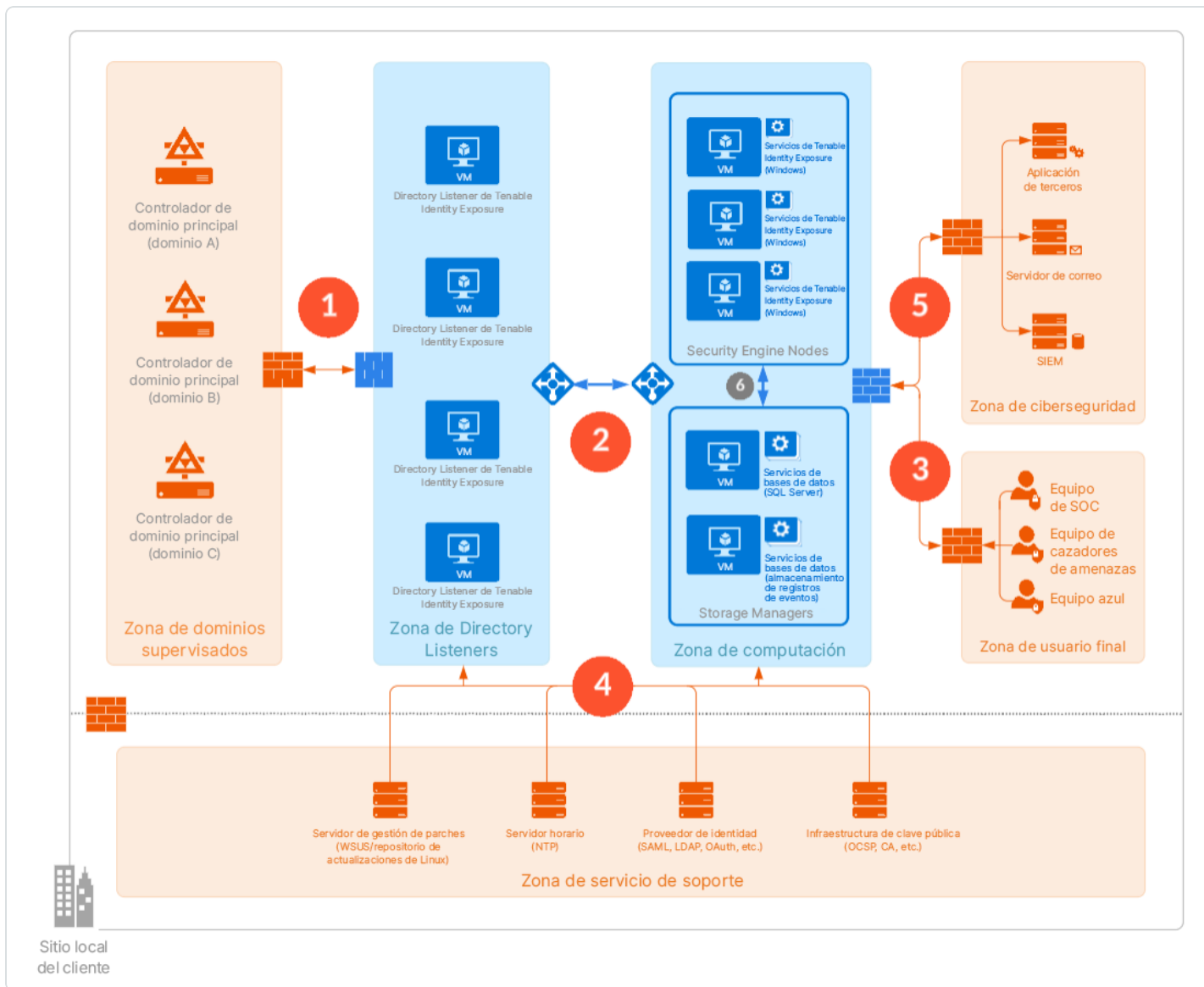
Además de estos flujos de red, se deben tener en cuenta otros flujos de red, por ejemplo:

- Acceso a los servicios para usuarios finales.
- Los flujos de red entre servicios de Tenable Identity Exposure.
- Los flujos de red desde los servicios de soporte que Tenable Identity Exposure utiliza, como la infraestructura de gestión de actualizaciones y el protocolo de tiempo de redes.

En el siguiente diagrama de la matriz de redes, encontrará más detalles sobre los diferentes servicios involucrados.







Protocolos obligatorios

En función de este diagrama, en la siguiente tabla se describe cada protocolo y puerto obligatorio que Tenable Identity Exposure utiliza.

Flujos de red	De	A	Uso de Tenable Identity Exposure	Tipo de tráfico	Protocolo y puerto
1.	Secure Relay de	Controladores de dominio	Directorio, replicación,	LDAP/LDAPS	TCP/389 y TCP/636



Tenable Identity Exposure	autenticación de usuarios y equipos, política de grupo, relaciones de confianza		ICMP/solicitud de eco ICMP/respuesta de eco
	Replicación, autenticación de usuarios y equipos, política de grupo, relaciones de confianza	SMB, CIFS, SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc	TCP/445
	Autenticación de usuarios y equipos, relaciones de confianza de nivel de bosque	Kerberos	TCP/88, TCP/464 y UDP/464
	Autenticación de usuarios y equipos, resolución de nombres, relaciones de confianza	DNS	UDP/53 y TCP/53
	Replicación, autenticación de usuarios y	RPC, DCOM, EPM, DRSUAPI, NetLogonR,	TCP dinámico (> 1024)



			equipos, política de grupo, relaciones de confianza	SamR, FRS	
			Directorio, replicación, autenticación de usuarios y equipos, política de grupo, relaciones de confianza	Catálogo global	TCP/3268 y TCP/3269
			Replicación	Asignador de puntos de conexión de RPC	TCP/135
2.	Secure Relay de Tenable Identity Exposure	Directory Listener de Tenable Identity Exposure	Flujos de API internas de Tenable Identity Exposure	HTTPS	TCP/443
			Actualizaciones automáticas	HTTP	TCP/5049
3.	Usuarios finales	Security Engine Node de Tenable Identity Exposure	Servicios para usuarios finales de Tenable Identity Exposure	HTTPS	TCP/443



			(portal web, API de REST, etc.)		
4.	Tenable Identity Exposure	Servicios de soporte	Sincronización de hora	NTP	UDP/123
			Infraestructura de actualización (por ejemplo, WSUS o SCCM)	HTTP/HTTPS	TCP/80 o TCP/443
			Infraestructura de PKI	HTTP/HTTPS	TCP/80 o TCP/443
			Proveedor de identidad Servidor SAML	HTTPS	TCP/443
			Proveedor de identidad LDAP	LDAP/LDAPS	TCP/389 y TCP/636
			Proveedor de identidad OAuth	HTTPS	TCP/443

Flujos adicionales

Además de los protocolos de Active Directory, ciertas configuraciones de Tenable Identity Exposure requieren flujos adicionales. Debe abrir estos protocolos y puertos entre Tenable Identity Exposure y el servicio de destino.

Flujos	De	A	Uso de Tenable	Tipo de	Protocolo y
--------	----	---	----------------	---------	-------------



de red		Identity Exposure (opcional)	tráfico	puerto	
5.	Secure Relay de Tenable Identity Exposure	Servicios de ciberseguridad	Notificaciones por correo electrónico	SMTP	TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025 (según la configuración del servidor SMTP)
			Notificaciones de SYSLOG	SYSLOG	TCP/601, TCP/6515, UDP/514 (según la configuración del servidor de registros de eventos)
			API de REST de Tenable	HTTP/TLS	TCP/443
	Controladores de dominio	Análisis con privilegios	Puertos RPC dinámicos	TCP/49152-65535, UDP/49152-65535	

Puertos internos

Si divide los servicios de Security Engine Node y Storage Manager en dos subredes diferentes, Tenable Identity Exposure requiere acceso a los siguientes puertos.



Nota: Para evitar problemas de rendimiento, Tenable recomienda no separar los servicios Security Engine Node y Storage Manager en redes diferentes.

Flujos de red	De	A	Uso de Tenable Identity Exposure	Tipo de tráfico	Protocolo y puerto
6.	Security Engine Node de Tenable Identity Exposure	Storage Manager de Tenable Identity Exposure	Acceso a bases de datos de MS SQL Server	Consultas de MS SQL	TCP/1433
			Acceso a la base de datos EventLogStorage	Consultas de EventLogStorage	TCP/4244
6.	Director y Listener de Tenable Identity Exposure	Security Engine Node de Tenable Identity Exposure	Bus de comunicación de Tenable Identity Exposure	Advanced Message Queuing Protocol	TCP/5671 y TCP/5672
			Flujos de API internas de Tenable Identity Exposure	HTTP/HTTPS	TCP/800 TCP/443
7.	Security Engine Node de Tenable Identity Exposure	Storage Manager de Tenable Identity Exposure	Acceso a bases de datos de MS SQL Server	Consultas de MS SQL	TCP/1433



	e		Acceso a la base de datos EventLogStorage	Consultas de EventLogStorage	TCP/4244
8.	Security Engine Node de Tenable Identity Exposure	Tenable Cloud <ul style="list-style-type: none">cloud.tenable.comsensor.cloud.tenable.com	Servicio en la nube de Tenable Identity Exposure	HTTPS	TCP/443

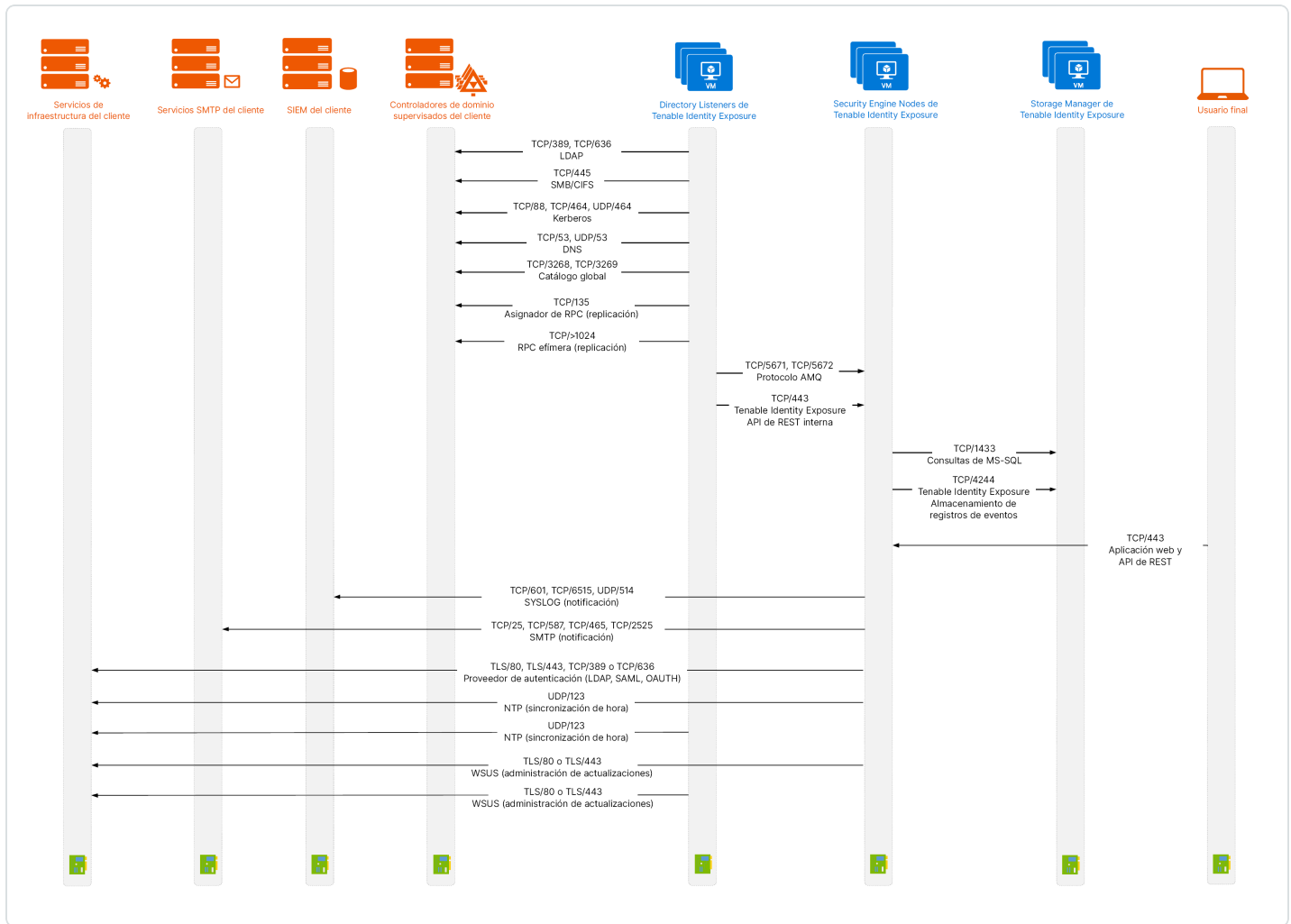
Servicios de soporte

Los servicios de soporte suelen depender mucho del proveedor o de la configuración. Por ejemplo, el servicio WSUS escucha de manera predeterminada en el puerto TCP/8530 para su versión 6.2 y superiores, pero en TCP/80 para otras versiones. Puede reconfigurar este puerto en cualquier otro puerto.

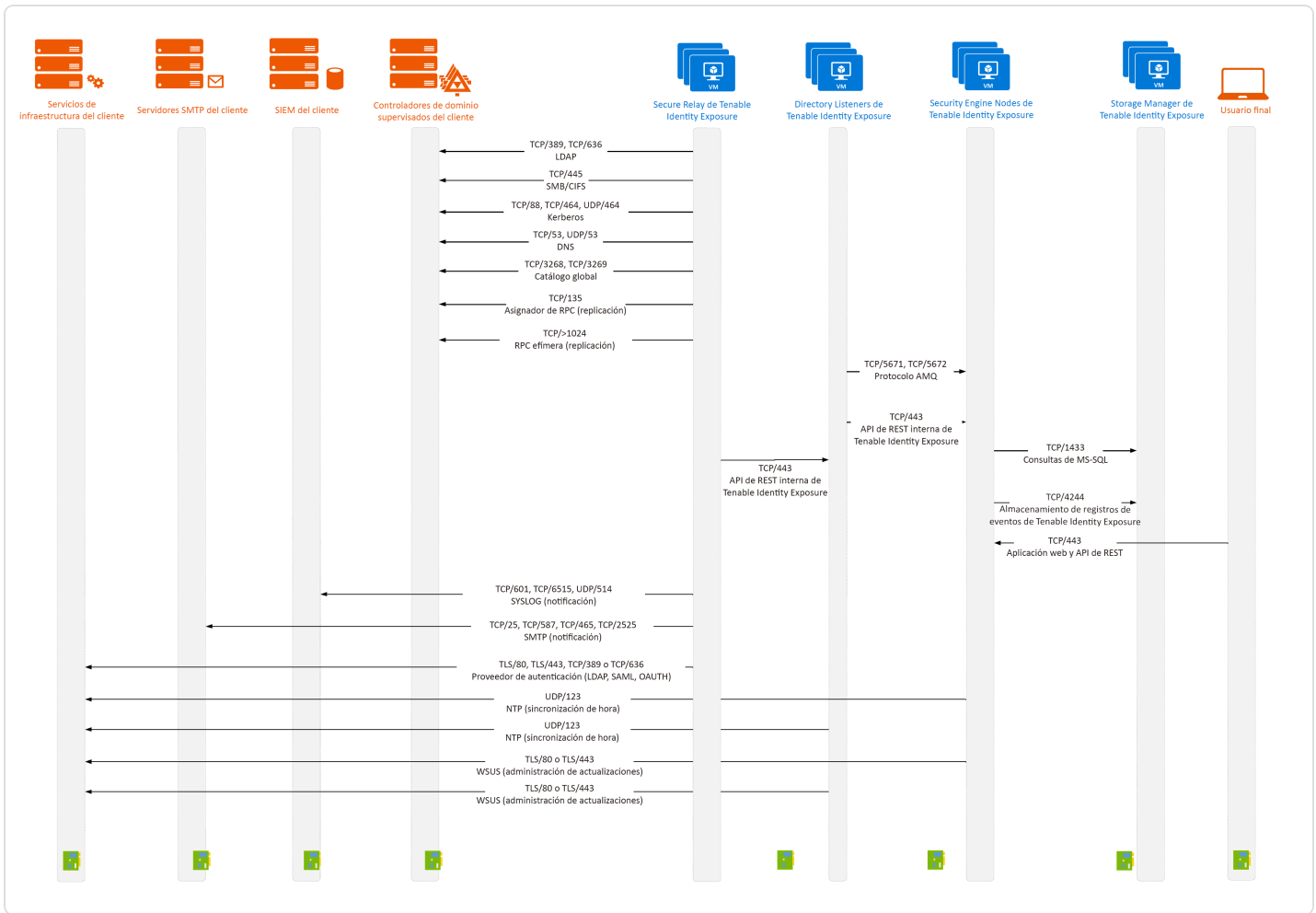
Compatibilidad con traducción de direcciones de red (NAT)

Tenable Identity Exposure inicia todas las conexiones de red, excepto las de los usuarios finales. Puede utilizar la traducción de direcciones de red (NAT) para conectarse a Tenable Identity Exposure a través de la interconexión de red.

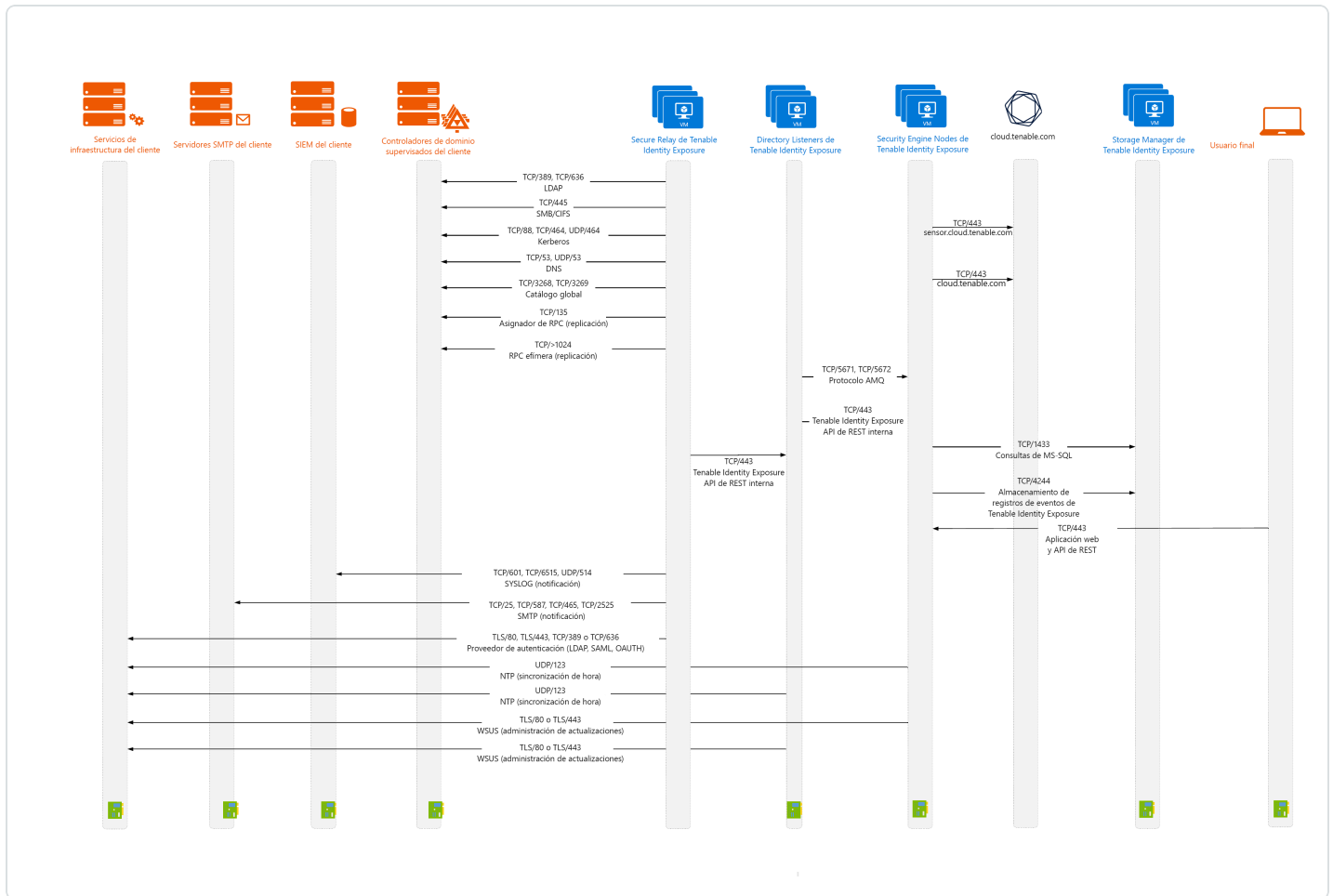
Plataforma local



Plataforma local mediante Secure Relay



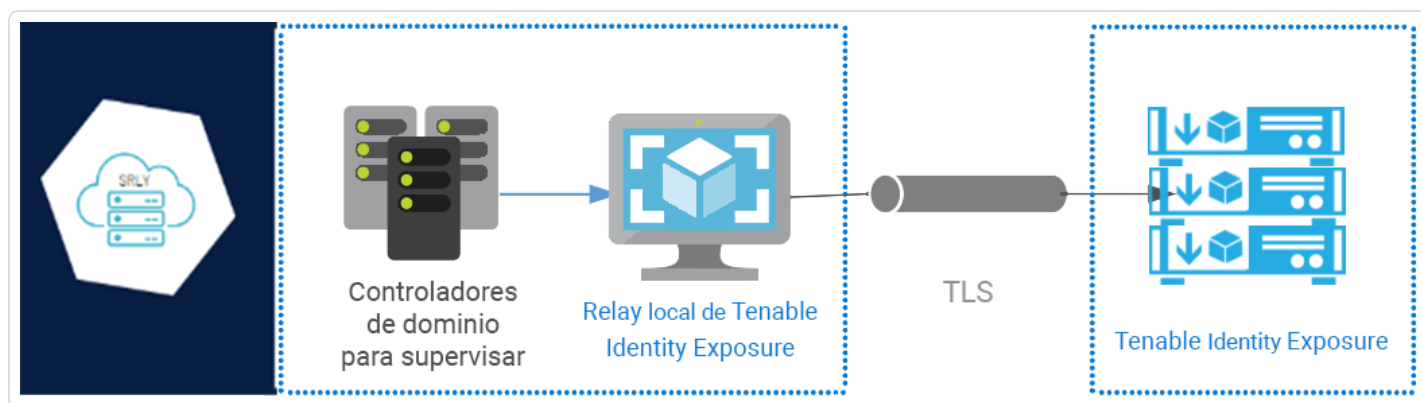
Plataforma local mediante Secure Relay con proxy



Requisitos de Secure Relay

Secure Relay es un modo de transferencia de datos de Active Directory desde su red a Tenable Identity Exposure mediante Seguridad de la capa de transporte (TLS) en lugar de una VPN, como se muestra en este diagrama. La funcionalidad Relay también admite proxy HTTP con o sin autenticación si la red requiere un servidor proxy para conectarse a internet.

Tenable Identity Exposure puede admitir varias instancias de Secure Relay que puede asignar a dominios según sus necesidades.



Requisitos de TLS

Para utilizar TLS 1.2, el servidor de Relay tiene que admitir al menos uno de los siguientes conjuntos de cifrado a partir del 24 de enero de 2024:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Además, asegúrese de que su configuración de Windows esté alineada con los conjuntos de cifrado especificados para la compatibilidad con la funcionalidad Relay.

Para comprobar si hay conjuntos de cifrado:

1. Ejecute el siguiente comando en PowerShell:

```
@("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
```

2. Consulte la salida: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256.



```
PS C:\Users> @"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256" | % { Get-TlsCipherSuite -Name $_ }

KeyType           : 0
Certificate        : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange           : ECDH
HashLength         : 0
Hash               :
CipherBlockLength  : 16
CipherLength       : 128
BaseCipherSuite    : 49199
CipherSuite        : 49199
Cipher             : AES
Name               : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Protocols          : {771, 65277}

KeyType           : 0
Certificate        : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange           : ECDH
HashLength         : 0
Hash               :
CipherBlockLength  : 16
CipherLength       : 256
BaseCipherSuite    : 49200
CipherSuite        : 49200
Cipher             : AES
Name               : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Protocols          : {771, 65277}
```

3. Una salida vacía indica que ninguno de los conjuntos de cifrado necesarios está habilitado para que la conexión TLS de Relay funcione. Habilite al menos un conjunto de cifrado.
4. Verifique la curva de criptografía de curva elíptica (ECC) desde el servidor de Relay. Esta verificación es obligatoria para usar conjuntos de cifrado Diffie-Hellman de curva elíptica efímero (ECDHE). Ejecute el siguiente comando en PowerShell:

```
Get-TlsEccCurve
```

5. Compruebe que tiene la curva **25519**. En caso contrario, habilítela.

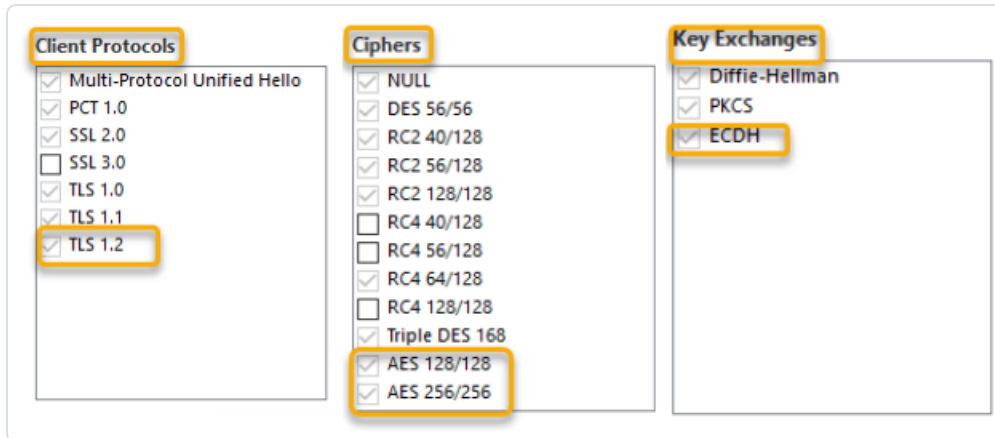
```
PS C:\Users> Get-TlsEccCurve
curve25519
NistP256
NistP384
```

Para verificar la configuración criptográfica de Windows:



1. En una herramienta IIS Crypto, compruebe tener habilitadas las siguientes opciones:

- Protocolos de cliente: **TLS 1.2**
- Cifrados: **AES 128/128** y **AES 256/256**
- Intercambios de claves: **ECDH**



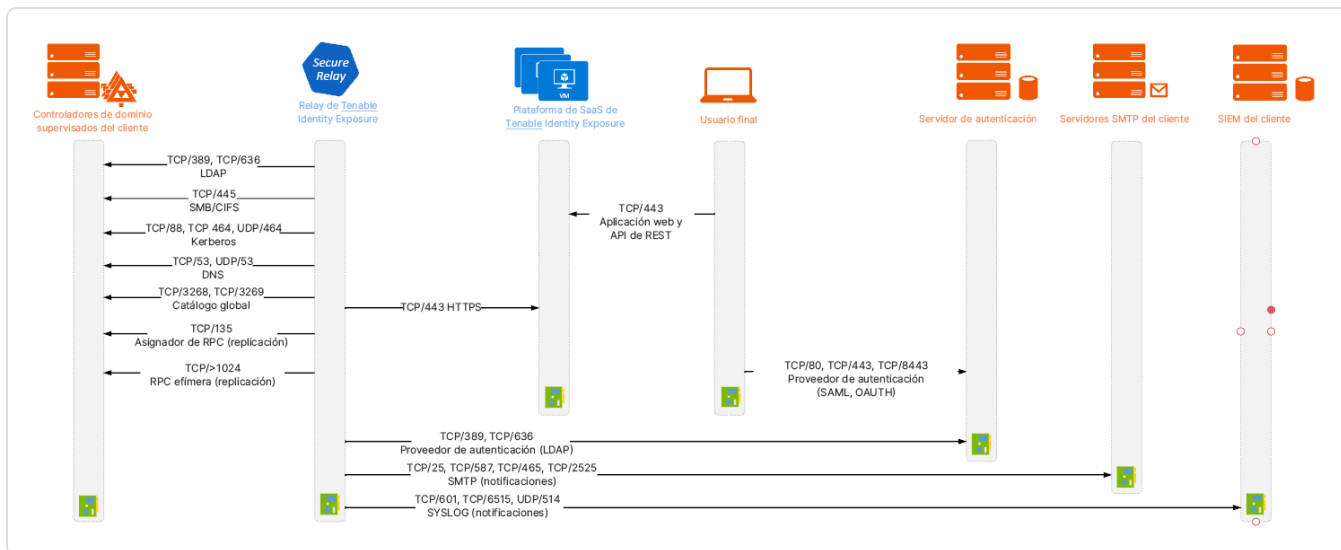
2. Después de modificar la configuración criptográfica, reinicie la máquina.

Nota: La modificación de la configuración criptográfica de Windows afecta a todas las aplicaciones que se ejecutan en la máquina y usan la biblioteca TLS de Windows, conocida como "Schannel". Por lo tanto, asegúrese de que cualquier ajuste que haga no cause efectos secundarios no deseados. Verifique que las configuraciones elegidas se alineen con los objetivos generales de endurecimiento de la organización o los mandatos de cumplimiento.

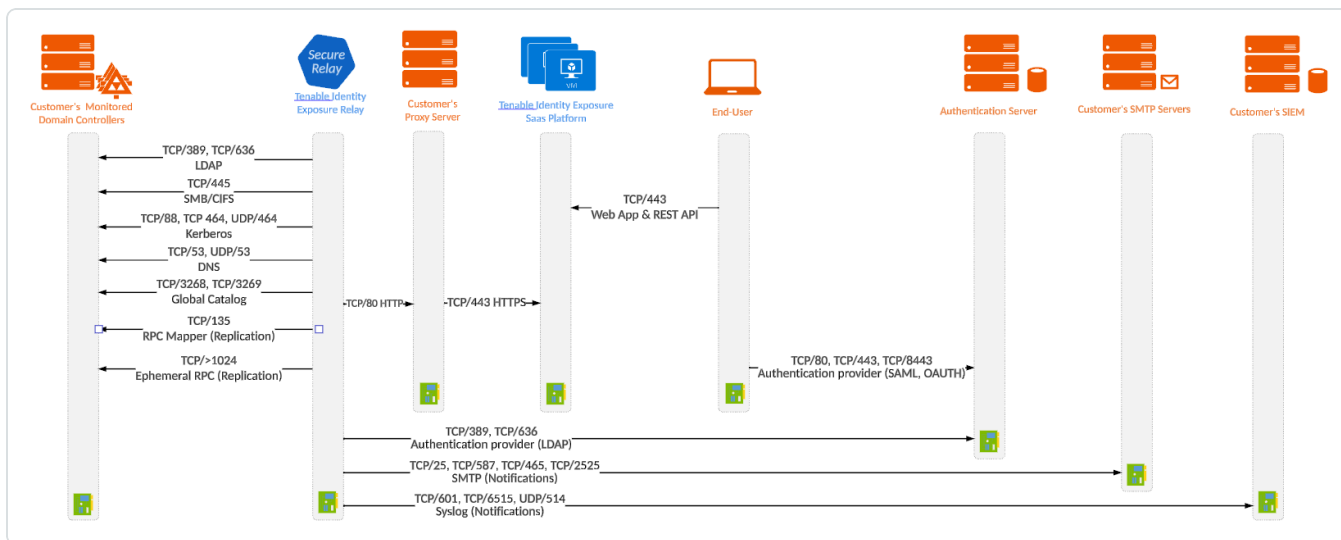
Puertos obligatorios



- Para una instalación clásica **sin un servidor proxy**, Relay requiere los siguientes puertos:



Para una instalación **con un servidor proxy**, Relay requiere los siguientes puertos:



Nota: Los flujos de red funcionan de la misma manera tanto para la plataforma local como para la de SaaS.

Requisitos previos de la máquina virtual

Los requisitos de la máquina virtual (VM) que aloja la instancia de Secure Relay son los siguientes:

Tamaño	Servicios de	Instancia	Memoria	vCPU	Topología	Espacio
--------	--------------	-----------	---------	------	-----------	---------



del cliente	Tenable Identity Exposure	obligatoria	(por instancia)	(por instancia)	de disco	disponible en disco (por instancia)
Cualquier tamaño	<ul style="list-style-type: none">• tenable_Relay• tenable_Envoy	1	8 GB de RAM	2 vCPU	Partición para registros independiente de la partición del sistema	30 GB

Nota: Si instala Secure Relay y Directory Listener en la misma máquina virtual, debe combinar los requisitos de tamaño. Consulte Resource Sizing.

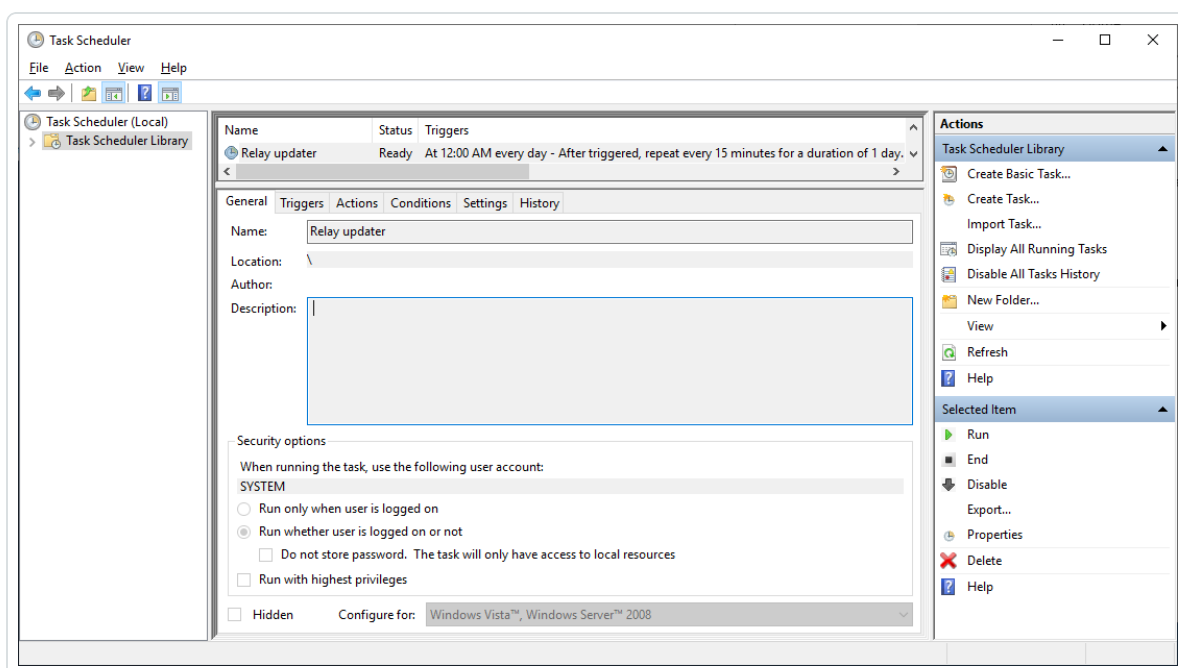
Sugerencia: Para la instalación inicial, es preferible que la VM no esté unida al dominio para evitar heredar políticas de GPO existentes que puedan interferir con el proceso de instalación. Después de completar la instalación, puede unir la VM al dominio.

Además, la VM debe tener:

- Tráfico HTTP o HTTPS: quite, deshabilite, omita o incluya en la whitelist cualquier cliente que pueda dirigir el tráfico HTTP o HTTPS hacia la máquina de Secure Relay. Esta acción bloquea la instalación de Secure Relay y detiene o ralentiza el tráfico que ingresa a la plataforma de Tenable.
- Un sistema operativo Windows Server 2016+ (no Linux).
- Consultas de DNS orientadas a internet y acceso a internet resueltos al menos para `cloud.tenable.com` y `*.tenable.ad` (TLS 1.2).
- Privilegios de administrador local.
- Configuración de EDR, antivirus y GPO:



- Suficiente CPU restante en la VM: por ejemplo, la característica Protección en tiempo real de Windows Defender consume una cantidad considerable de CPU y puede saturar la máquina.
- Actualizaciones automáticas:
 - Permita las llamadas hacia *.tenable.ad para que la funcionalidad de actualizaciones automáticas pueda descargar un archivo ejecutable de Relay.
 - Compruebe que no haya ningún objeto de política de grupo (GPO) que bloquee la funcionalidad de actualizaciones automáticas.
 - No elimine ni modifique la tarea programada “Actualizador de Relay”:



Archivos y procesos permitidos

Para que Relay funcione sin problemas, permita ciertos archivos y procesos de herramientas de seguridad de terceros, como antivirus o EDR (detección y respuesta de puntos de conexión) y XDR (detección y respuesta extendidas).

Nota: Adapte la ruta C:\ a la unidad de instalación de Relay.

Windows



Archivos
C:\Tenable*
C:\tools*
C:\ProgramData\Tenable*
Procesos
nssm.exe --> Ruta: C:\tools\nssm.exe
Tenable.Relay.exe --> Ruta: C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe
envoy.exe --> Ruta: C:\Tenable\Tenable.ad\SecureRelay\envoy.exe
updater.exe --> Ruta: C:\Tenable\Tenable.ad\updater.exe
powershell.exe --> Ruta: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (puede diferir según la versión del SO)
Tareas programadas
C:\Windows\System32\Tasks\Relay updater
C:\Windows\System32\Tasks\Manual Renew Apikey
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\CompressLogsSecureRelay
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\RemoveLogsSecureRelay
Clave del registro
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad Secure Relay

Requisitos del portal web

Tenable Identity Exposure no requiere ninguna configuración ni plug-in específicos de los navegadores del cliente.

Navegadores de Internet admitidos

Debe utilizar la versión más reciente de un navegador web admitido.



Navegadores web admitidos, incluida la versión mínima	
Microsoft	Edge, versión 38.14393, o Internet Explorer 11
Google	Chrome, versión 56.0.2924
Mozilla	Firefox, versión 52.7.3
Apple	Safari, versión 11.0

Certificado del servidor TLS

Tenable Identity Exposure utiliza el mecanismo de cifrado SSL/TLS para acceder a la aplicación.

Tenable recomienda encarecidamente utilizar un certificado válido que se proporcione durante la instalación.

Configuración y versión de TLS admitidas

- De TLS 1.1 a TLS 1.3
- Certificado autofirmado de Tenable
- Certificado emitido desde la PKI privada
- Certificado TLS alternativo

Configuración y versión de TLS recomendadas

- TLS 1.2
- Certificado emitido desde la PKI privada

Actualización de certificados TLS

Si tiene que cambiar los certificados TLS más allá de una actualización, puede actualizar los archivos CRT y de claves en `Tenable\Tenable.ad\Certificates` y reiniciar los servicios.

Consulte también

- [HTTPS for Tenable Identity Exposure Web Application](#)

Integración en un dominio de Active Directory



Tenable Identity Exposure se ejecuta en sistemas operativos Microsoft Server que se conectan a un dominio de Active Directory (AD). Las siguientes son pautas sobre si se deben conectar o no estos servidores a un dominio de AD.

- Debido a que Tenable Identity Exposure ofrece información de seguridad confidencial, **no se recomienda unir servidores de Tenable a ningún dominio de AD**. De hecho, trabajar en un entorno aislado permite una clara separación entre el perímetro supervisado y la entidad supervisora (es decir, Tenable Identity Exposure). En esta configuración, un atacante con acceso inicial o privilegios limitados en el dominio supervisado no puede acceder directamente a Tenable Identity Exposure y a los resultados de análisis de seguridad.
- Si tiene una infraestructura confiable, puede elegir ejecutar Tenable Identity Exposure en servidores unidos a dominios. Este enfoque mejora la gestión de los servidores, ya que es parte del proceso normal que se sigue para cada servidor unido a un dominio. En particular, los servidores de Tenable Identity Exposure aplican las mismas políticas de endurecimiento que cualquier otro servidor corporativo. Tenable recomienda esta arquitectura solo en entornos de AD seguros y debe tener en cuenta los siguientes riesgos en caso de que una instancia de AD esté en peligro:
 - Un atacante con privilegios de administración de servidores puede recopilar más información sobre las formas de poner el sistema en peligro mediante el análisis de datos de Tenable Identity Exposure.
 - La política de seguridad en servidores unidos a dominios puede prohibir el acceso administrativo otorgado a Soporte de Tenable o sus socios certificados.
 - Un ataque puede ocultar un incidente de seguridad para vulnerar la supervisión de seguridad de Tenable Identity Exposure.

Secure Relay de Tenable Identity Exposure

A partir de la versión 3.59, el componente **Secure Relay** se encarga de las tareas designadas en la plataforma de Tenable Identity Exposure:

- Le permite configurar dominios desde los cuales reenvía los datos al componente Directory Listener (DL) que recopila objetos de AD.



- Facilita la configuración y el mantenimiento de grandes infraestructuras a través de actualizaciones automáticas: ya no se necesitan varios DL que requieran actualizaciones simultáneas.
- Sirve como puente entre el DL único y varios puntos de conexión, como controladores de dominio o servidores SMTP, SYSLOG o LDAP para la autenticación dentro del producto.
- Se enlaza a uno o varios dominios. El DL puede gestionar una cantidad ilimitada de instancias de Relay.
- Requiere configuración en la consola de Tenable Identity Exposure, como conversiones de nomenclatura y asignaciones (dominio, SMTP, SYSLOG, autenticación LDAP).

Antes de empezar

Siga estas pautas para la instalación o actualización a Tenable Identity Exposure 3.59 con Secure Relay:

1. Revise [Requisitos de Secure Relay](#).
2. **Requisitos de red:**
 - En versiones anteriores y actuales, el DL se comunicaba directamente con el SEN mediante el protocolo AMQP(S).
 - En la versión 3.59, las instancias de Relay que reemplazan a varios DL se comunican con el único DL restante a través de HTTPS.
 - Envoy es el proxy inverso.
3. **Clave de vinculación:** la instalación de Secure Relay requiere una clave de vinculación de un solo uso que contiene la dirección de la red y un token de autenticación. Tenable Identity Exposure vuelve a generar una nueva clave después de cada instalación correcta de Secure Relay.

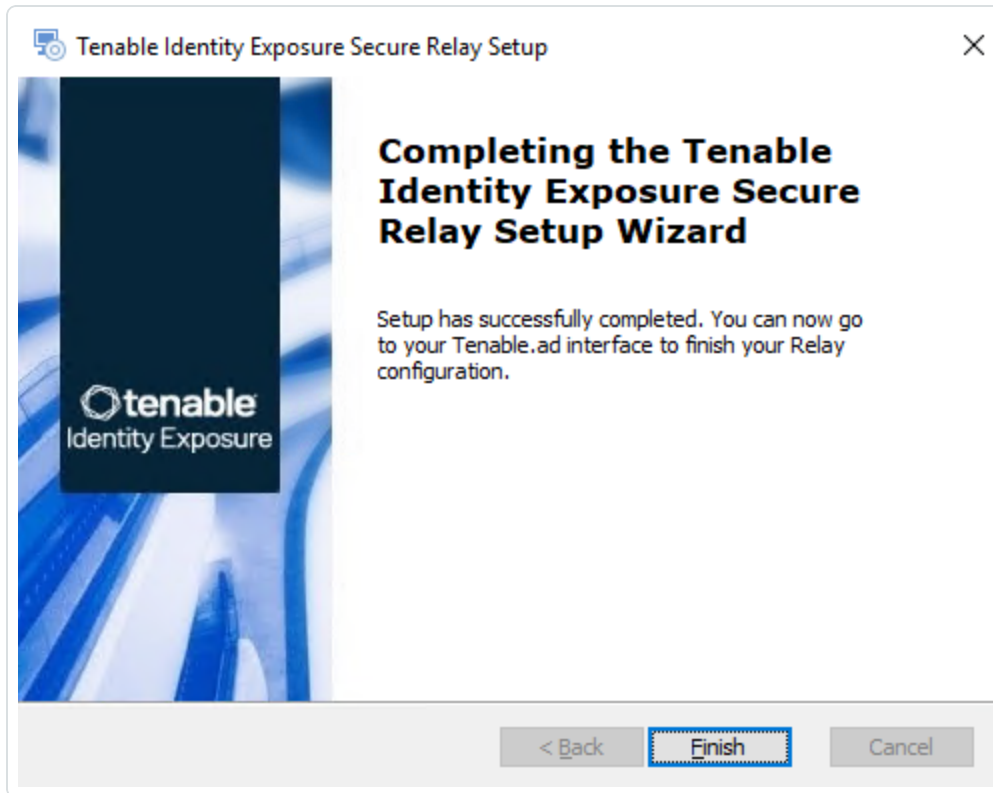
Para recuperar la clave de vinculación:

1. En la consola de Tenable Identity Exposure, haga clic en **Sistema** en la barra de menú de la izquierda y seleccione la pestaña **Configuración > Relay**.



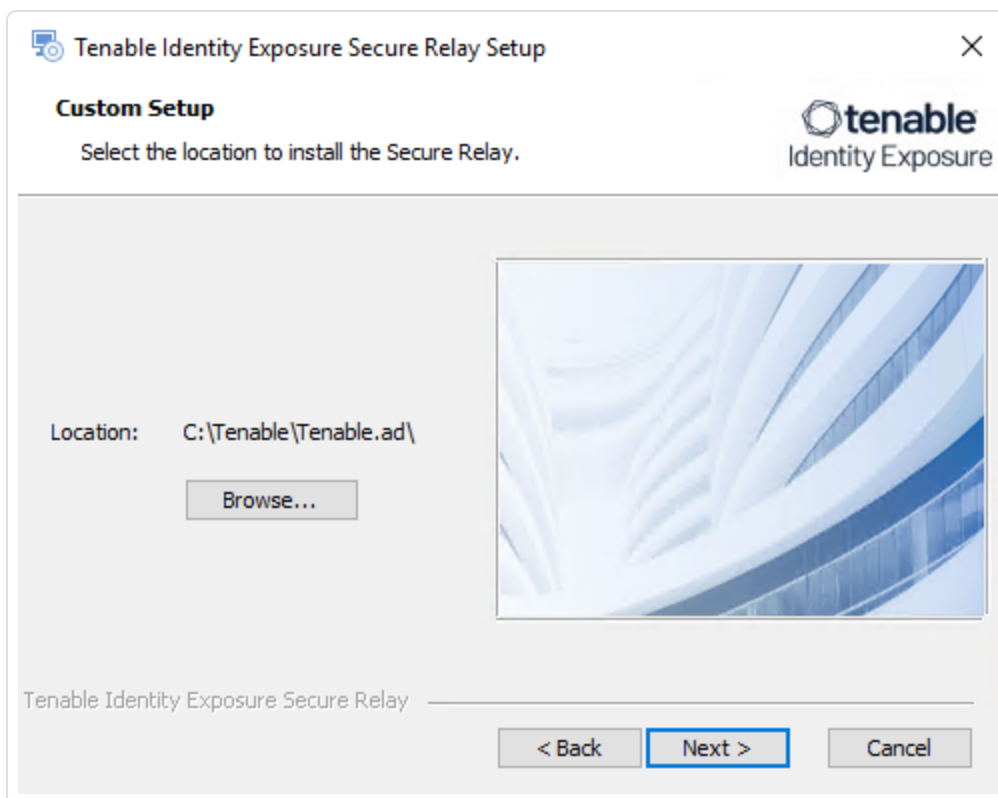
1. Descargue el programa ejecutable de Secure Relay del [sitio de descargas de Tenable](#).
2. Haga doble clic en el archivo `tenable.ad_SecureRelay_v3.xx.x` para iniciar el asistente de instalación.

Aparece la pantalla de **Bienvenida**.



3. Haga clic en **Siguiente**.

Aparece la ventana **Instalación personalizada**.



4. Haga clic en **Explorar** para seleccionar la partición de disco que reservó para Secure Relay (independiente de la partición del sistema).
5. Haga clic en **Siguiente**.

Aparece la ventana **Configuración de Relay**.

Tenable Identity Exposure Secure Relay Setup

Relay Configuration
Complete the required information.

Relay Name SR-01

Linking Key i2tlbiI6IkNGM0I1NkrFLUE3RUQtNDk0QS05MjJFLTk2Rjk3OTc2QTBCOSJ9

You can retrieve the linking key from your Tenable Identity Exposure user interface (System > Configuration > Relay).

Link: [How to get your linking key](#)

Tenable Identity Exposure Secure Relay

< Back Next > Cancel

6. Proporcione la siguiente información:

- En el cuadro **Nombre de Relay**, escriba un nombre para la instancia de Secure Relay.
- En el cuadro **Clave de vinculación**, pegue la clave de vinculación que recuperó del portal de Tenable Identity Exposure.
- Si elige usar un servidor proxy, seleccione la opción **Usar un proxy HTTP para las llamadas a Relay** e indique la dirección y el número de puerto del proxy.

7. Haga clic en **Siguiente**.

Aparece la ventana "Configuración del proxy":

The screenshot shows a dialog box titled "Tenable Identity Exposure Secure Relay Setup" with a close button (X) in the top right corner. Below the title bar, the text "Proxy Configuration" is displayed, followed by the instruction "Complete the required information." and the Tenable Identity Exposure logo. The main area contains five input fields: "Proxy Type" (a dropdown menu currently set to "None"), "Proxy Address", "Proxy Port", "User", and "Password". At the bottom, there is a "Test Connectivity" button with a green indicator light, and three navigation buttons: "< Back", "Next >", and "Cancel".

8. Seleccione una de las siguientes opciones:

- a. **Ninguno:** no se usa un servidor proxy.
- b. **Sin autenticación:** escriba la dirección y el puerto del servidor proxy.
- c. **Autenticación básica:** además de la dirección y el puerto, escriba el usuario y la contraseña del servidor proxy.

Precaución: Para configurar un proxy con la opción "Sin autenticación" o "Autenticación básica", Relay solo admite direcciones IPv4 (como 192.168.0.1) o un URI de proxy sin http:// ni https:// (como miproxy.miempresa.com). Relay no admite direcciones IPv6 (como 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

9. Haga clic en **Probar la conectividad**. Puede ocurrir lo siguiente:

- **Luz verde:** la conexión se estableció correctamente.
- **Clave de vinculación no válida:** recupere la clave de vinculación del portal de Tenable Identity Exposure.



- **Nombre de Relay no válido:** este cuadro no puede quedar vacío. Escriba un nombre de Relay.
- **Error de conexión:** verifique el acceso a internet.

10. Haga clic en **Siguiente**.

Aparece la ventana **Listo para instalar**.

11. Haga clic en **Instalar**.

12. Una vez completada la instalación, haga clic en **Finalizar**.

Verificaciones posteriores a la instalación

Una vez completada la instalación de Secure Relay, compruebe lo siguiente:

Lista de instancias de Relay instaladas en Tenable Identity Exposure

Para ver la lista de instancias de Relay instaladas:

- En Tenable Identity Exposure, haga clic en **Sistema** en la barra de menú de la izquierda y seleccione la pestaña **Gestión de Relay**.

En el panel se muestra una lista de instancias de Secure Relay y sus dominios vinculados.

Servicios

Después de una instalación correcta, se ejecutan los siguientes servicios:

- Tenable_Relay
- tenable_envoy

Nota: Puede encontrar la licencia de Envoy en Tenable Identity Exposure en **Sistema > Información legal > Licencia de Envoy**.

Variables de entorno

La instalación también agregó cuatro nuevas variables de entorno relacionadas con Secure Relay con nombres que comienzan por "TENABLE". Si eligió usar un servidor proxy, hay dos variables adicionales relacionadas con la IP y el puerto del proxy.

Registros para solucionar problemas



Puede encontrar registros en las siguientes ubicaciones:

- **Registros de instalación:** C:\Users\\AppData\Local\Temp
- **Registros de Relay:** en la VM que aloja Secure Relay, en la carpeta especificada en el momento de la instalación.

Configuración de Relay

- [Configurar Relay](#)

Actualizaciones automáticas


Después de instalar Secure Relay, Tenable Identity Exposure busca nuevas versiones periódicamente. Este proceso está totalmente automatizado y requiere acceso HTTPS a su dominio (TCP/443). Un ícono en la bandeja de red indica cuándo Tenable Identity Exposure está actualizando Secure Relay. Una vez que se completa el proceso, los servicios de Tenable Identity Exposure se reinician y se reanuda la recopilación de datos.

Desinstalación

Para desinstalar Secure Relay:

1. En Windows, vaya a **Configuración > Aplicaciones y características > Secure Relay de Tenable Identity Exposure**.
2. Haga clic en **Desinstalar**.

Cuando se complete la desinstalación, los servicios y las variables de entorno de Secure Relay de Tenable Identity Exposure ya no aparecerán en el sistema.

3. En Tenable Identity Exposure, haga clic en **Sistema** en la barra de menú de la izquierda y seleccione la pestaña **Gestión de Relay**.
4. Seleccione la instancia de Relay que acaba de desinstalar y haga clic en  para quitarla de la lista de instancias de Relay disponibles.

Consulte también

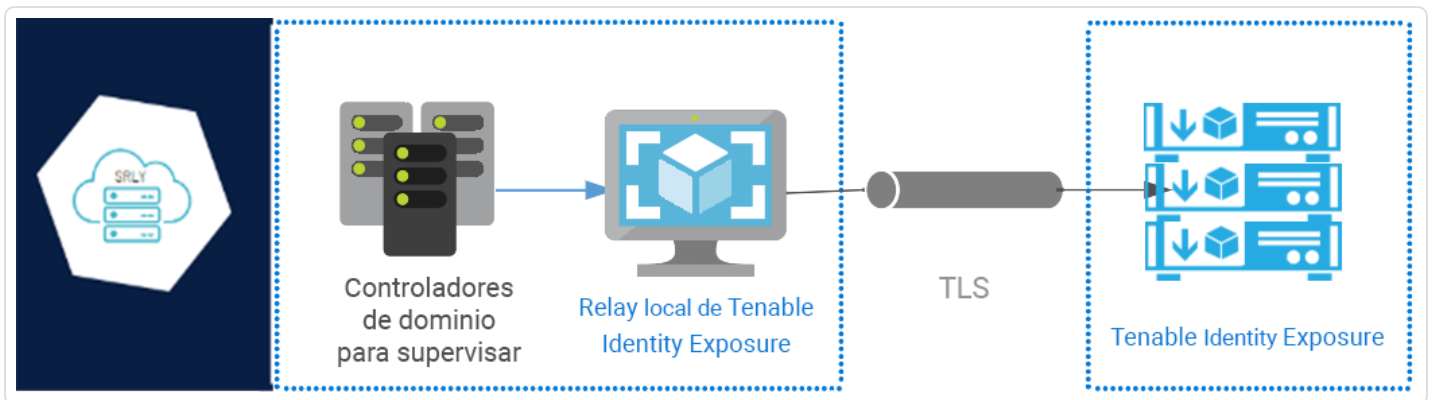
- [Solucionar problemas de instalación de Secure Relay](#)



Requisitos de Secure Relay

Secure Relay es un modo de transferencia de datos de Active Directory desde su red a Tenable Identity Exposure mediante Seguridad de la capa de transporte (TLS) en lugar de una VPN, como se muestra en este diagrama. La funcionalidad Relay también admite proxy HTTP con o sin autenticación si la red requiere un servidor proxy para conectarse a internet.

Tenable Identity Exposure puede admitir varias instancias de Secure Relay que puede asignar a dominios según sus necesidades.



Requisitos de TLS

Para utilizar TLS 1.2, el servidor de Relay tiene que admitir al menos uno de los siguientes conjuntos de cifrado a partir del 24 de enero de 2024:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Además, asegúrese de que su configuración de Windows esté alineada con los conjuntos de cifrado especificados para la compatibilidad con la funcionalidad Relay.

Para comprobar si hay conjuntos de cifrado:



1. Ejecute el siguiente comando en PowerShell:

```
@("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
```

2. Consulte la salida: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256.

```
PS C:\Users> @("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
```

KeyType	: 0
Certificate	: RSA
MaximumExchangeLength	: 65536
MinimumExchangeLength	: 0
Exchange	: ECDH
HashLength	: 0
Hash	:
CipherBlockLength	: 16
CipherLength	: 128
BaseCipherSuite	: 49199
CipherSuite	: 49199
Cipher	: AES
Name	: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Protocols	: {771, 65277}

KeyType	: 0
Certificate	: RSA
MaximumExchangeLength	: 65536
MinimumExchangeLength	: 0
Exchange	: ECDH
HashLength	: 0
Hash	:
CipherBlockLength	: 16
CipherLength	: 256
BaseCipherSuite	: 49200
CipherSuite	: 49200
Cipher	: AES
Name	: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Protocols	: {771, 65277}

3. Una salida vacía indica que ninguno de los conjuntos de cifrado necesarios está habilitado para que la conexión TLS de Relay funcione. Habilite al menos un conjunto de cifrado.
4. Verifique la curva de criptografía de curva elíptica (ECC) desde el servidor de Relay. Esta verificación es obligatoria para usar conjuntos de cifrado Diffie-Hellman de curva elíptica efímero (ECDHE). Ejecute el siguiente comando en PowerShell:

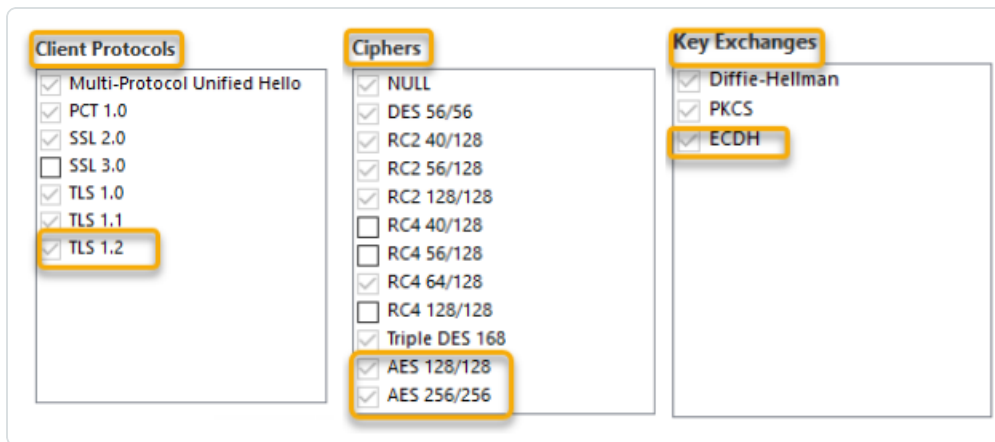
```
Get-TlsEccCurve
```

5. Compruebe que tiene la curva **25519**. En caso contrario, habilítela.


```
PS C:\Users> Get-TlsEccCurve
curve25519
NistP256
NistP384
```

Para verificar la configuración criptográfica de Windows:

1. En una herramienta IIS Crypto, compruebe tener habilitadas las siguientes opciones:
 - Protocolos de cliente: **TLS 1.2**
 - Cifrados: **AES 128/128** y **AES 256/256**
 - Intercambios de claves: **ECDH**



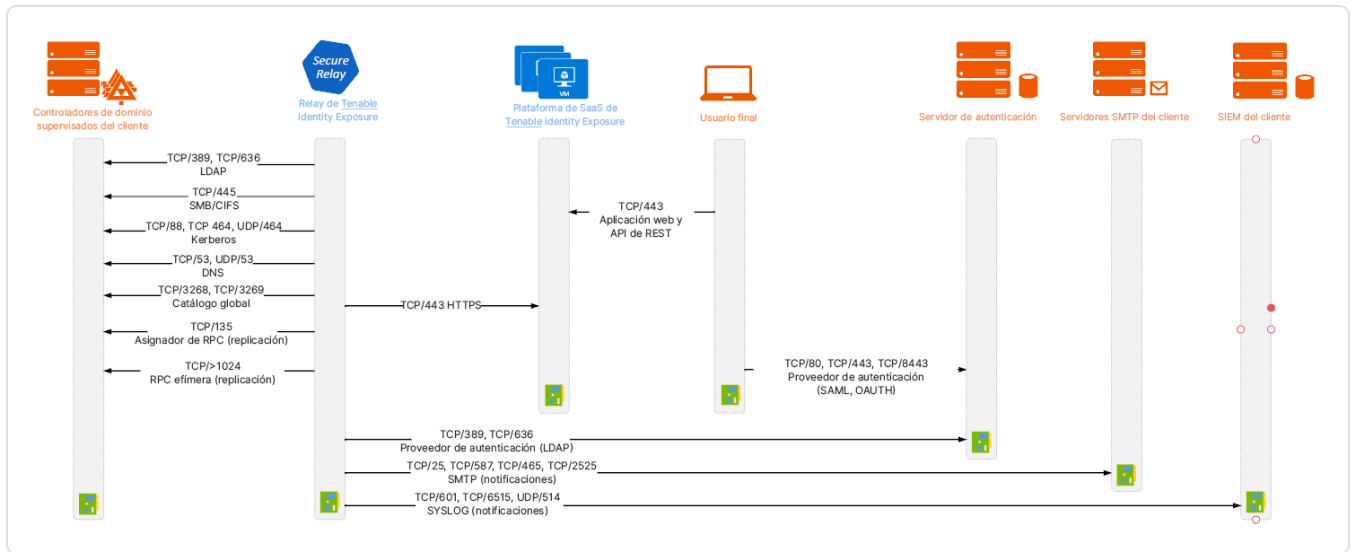
2. Después de modificar la configuración criptográfica, reinicie la máquina.

Nota: La modificación de la configuración criptográfica de Windows afecta a todas las aplicaciones que se ejecutan en la máquina y usan la biblioteca TLS de Windows, conocida como "Schannel". Por lo tanto, asegúrese de que cualquier ajuste que haga no cause efectos secundarios no deseados. Verifique que las configuraciones elegidas se alineen con los objetivos generales de endurecimiento de la organización o los mandatos de cumplimiento.

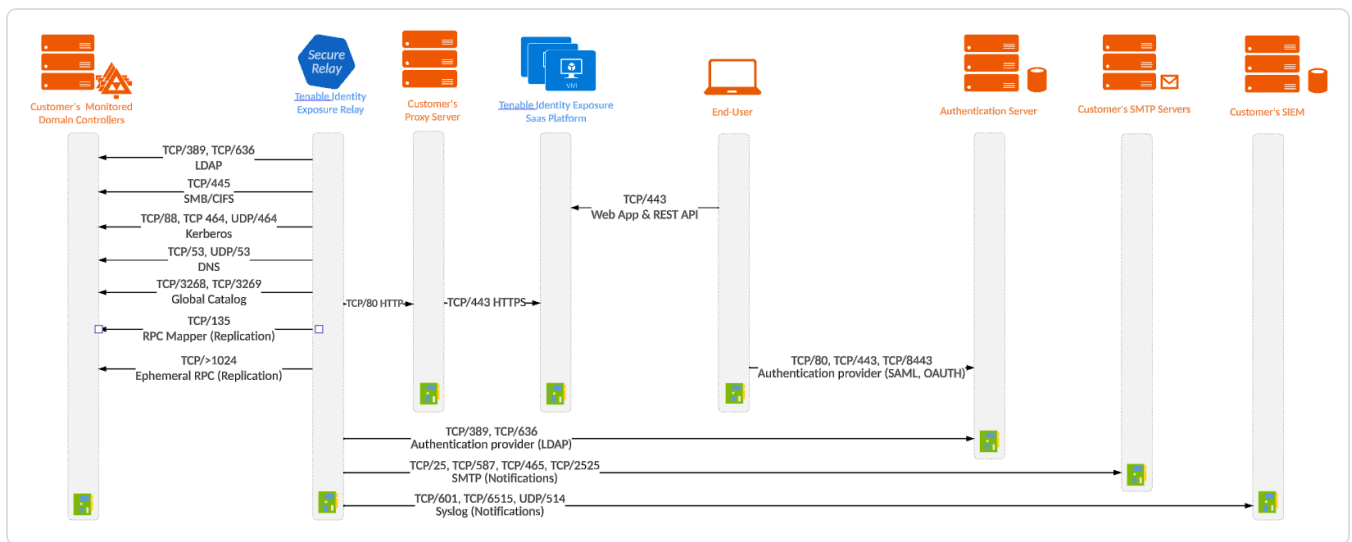
Puertos obligatorios



- Para una instalación clásica **sin un servidor proxy**, Relay requiere los siguientes puertos:



Para una instalación **con un servidor proxy**, Relay requiere los siguientes puertos:



Nota: Los flujos de red funcionan de la misma manera tanto para la plataforma local como para la de SaaS.

Requisitos previos de la máquina virtual

Los requisitos de la máquina virtual (VM) que aloja la instancia de Secure Relay son los siguientes:

Tamaño	Servicios de	Instancia	Memoria	vCPU	Topología	Espacio
--------	--------------	-----------	---------	------	-----------	---------



del cliente	Tenable Identity Exposure	obligatoria	(por instancia)	(por instancia)	de disco	disponible en disco (por instancia)
Cualquier tamaño	<ul style="list-style-type: none">• tenable_Relay• tenable_Envoy	1	8 GB de RAM	2 vCPU	Partición para registros independiente de la partición del sistema	30 GB

Nota: Si instala Secure Relay y Directory Listener en la misma máquina virtual, debe combinar los requisitos de tamaño. Consulte Resource Sizing.

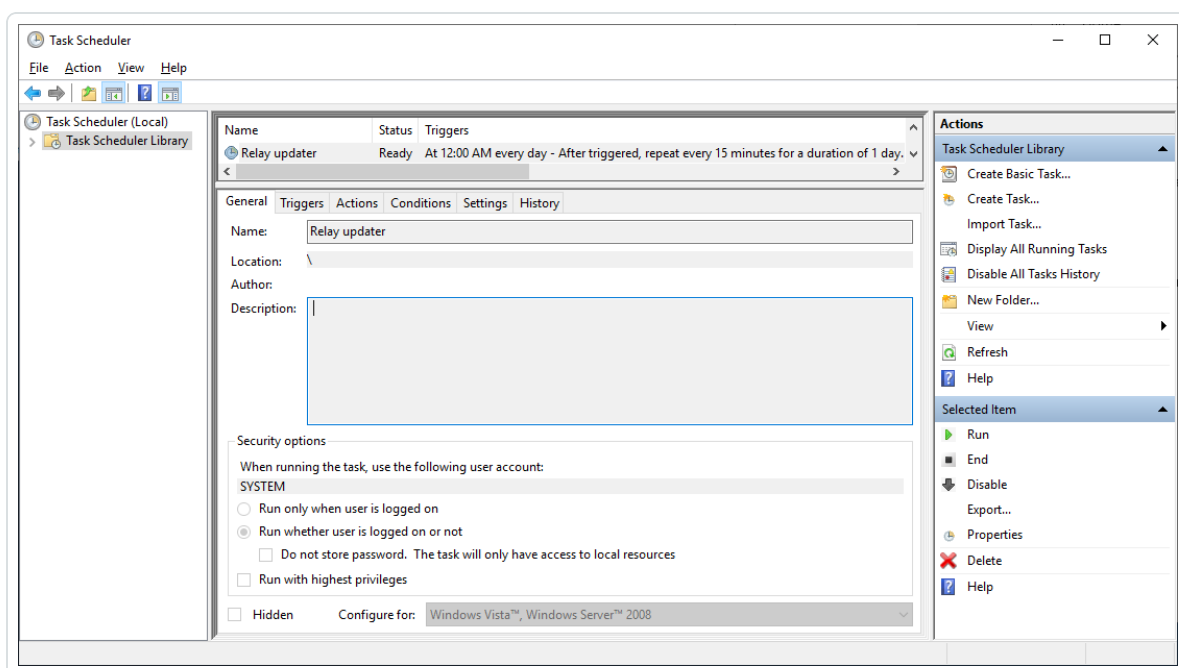
Sugerencia: Para la instalación inicial, es preferible que la VM no esté unida al dominio para evitar heredar políticas de GPO existentes que puedan interferir con el proceso de instalación. Después de completar la instalación, puede unir la VM al dominio.

Además, la VM debe tener:

- Tráfico HTTP o HTTPS: quite, deshabilite, omita o incluya en la whitelist cualquier cliente que pueda dirigir el tráfico HTTP o HTTPS hacia la máquina de Secure Relay. Esta acción bloquea la instalación de Secure Relay y detiene o ralentiza el tráfico que ingresa a la plataforma de Tenable.
- Un sistema operativo Windows Server 2016+ (no Linux).
- Consultas de DNS orientadas a internet y acceso a internet resueltos al menos para `cloud.tenable.com` y `*.tenable.ad` (TLS 1.2).
- Privilegios de administrador local.
- Configuración de EDR, antivirus y GPO:



- Suficiente CPU restante en la VM: por ejemplo, la característica Protección en tiempo real de Windows Defender consume una cantidad considerable de CPU y puede saturar la máquina.
- Actualizaciones automáticas:
 - Permita las llamadas hacia *.tenable.ad para que la funcionalidad de actualizaciones automáticas pueda descargar un archivo ejecutable de Relay.
 - Compruebe que no haya ningún objeto de política de grupo (GPO) que bloquee la funcionalidad de actualizaciones automáticas.
 - No elimine ni modifique la tarea programada “Actualizador de Relay”:



Archivos y procesos permitidos

Para que Relay funcione sin problemas, permita ciertos archivos y procesos de herramientas de seguridad de terceros, como antivirus o EDR (detección y respuesta de puntos de conexión) y XDR (detección y respuesta extendidas).

Nota: Adapte la ruta C:\ a la unidad de instalación de Relay.

Windows



Archivos
C:\Tenable*
C:\tools*
C:\ProgramData\Tenable*
Procesos
nssm.exe --> Ruta: C:\tools\nssm.exe
Tenable.Relay.exe --> Ruta: C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe
envoy.exe --> Ruta: C:\Tenable\Tenable.ad\SecureRelay\envoy.exe
updater.exe --> Ruta: C:\Tenable\Tenable.ad\updater.exe
powershell.exe --> Ruta: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (puede diferir según la versión del SO)
Tareas programadas
C:\Windows\System32\Tasks\Relay updater
C:\Windows\System32\Tasks\Manual Renew Apikey
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\CompressLogsSecureRelay
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\RemoveLogsSecureRelay
Clave del registro
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad Secure Relay


Configurar Relay

Después de la instalación y las verificaciones posteriores a la instalación, configure Relay en Tenable Identity Exposure para vincularlo a un dominio y establecer alertas.

- Asignación de dominio: reemplace las opciones de aplicaciones de varios DL o las variables de entorno de red por las opciones de dominios necesarias (la cantidad de modificaciones puede variar).

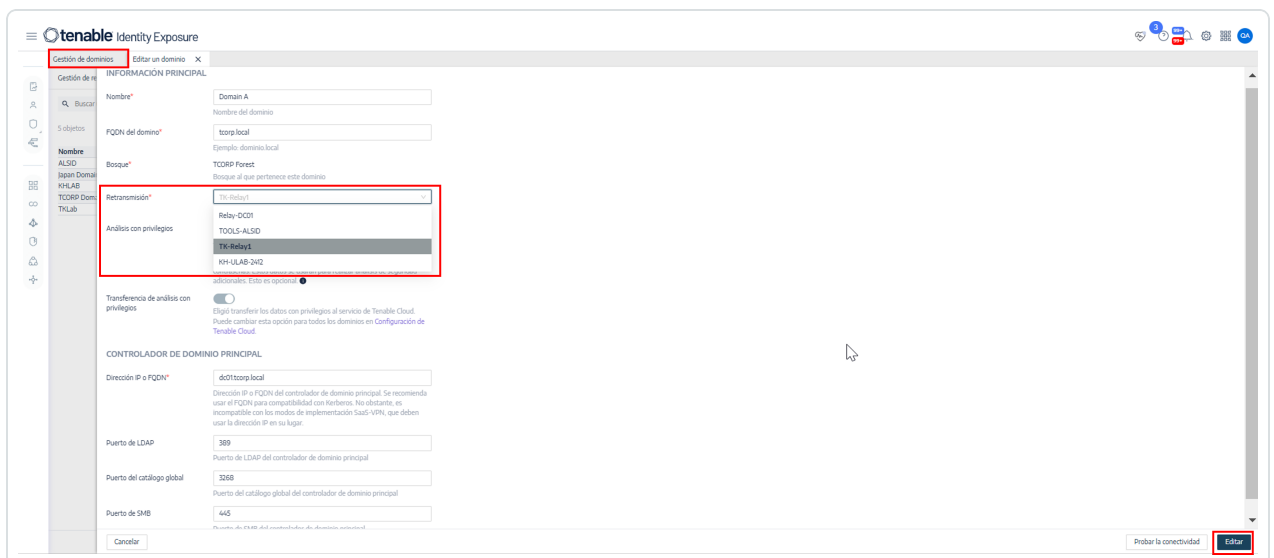


Para asignar un dominio a una instancia de Secure Relay:

1. En Tenable Identity Exposure, haga clic en **Sistema** en la barra de menú de la izquierda y seleccione la pestaña **Gestión de dominios**.
2. En la lista de dominios, seleccione un dominio que quiera vincular y haga clic en  al final de la línea.

Se abre el panel **Editar un dominio**.

3. En el cuadro **Relay**, haga clic en la flecha para mostrar una lista desplegable de instancias de Relay instaladas y seleccione una instancia de Relay para vincularla al dominio.



Haga clic en **Editar**.

Un mensaje confirma que Tenable Identity Exposure actualizó el dominio. SYSVOL y LDAP se sincronizan para incluir la modificación. Trail Flow comienza a recibir nuevos eventos.

- Asignación de alertas:
 - Configuración de SMTP: haga los cambios necesarios en [Configuración de servidores SMTP](#).



- Alertas de SYSLOG: configure [Alertas de SYSLOG](#) (la cantidad de modificaciones puede variar).
- Asignación de LDAP: implemente la [Autenticación mediante LDAP](#).

Instalar Secure Relay (CLI)

En el siguiente procedimiento se instala Secure Relay mediante la línea de comandos. Antes de comenzar, compruebe que cumple con los requisitos previos necesarios y tiene la **clave de vinculación obligatoria**, como se describe en [Secure Relay de Tenable Identity Exposure](#).

Para instalar Secure Relay mediante la CLI:

1. Descargue el instalador del [portal de descargas de Tenable Identity Exposure](#) en la VM.
2. En PowerShell, ejecute el siguiente comando:

```
Instalación de Secure Relay
```

```
<PATH>\tenable.ad_SecureRelay_v3.43.0.exe /qn OPTIONS
```

Con las siguientes opciones:

- APPDIR=<ruta> (obligatorio): ruta a la carpeta de instalación de Relay. Elija una partición que no sea la partición Sistema, ya que Relay crea archivos de registros grandes.
- EDIT_LINKINGKEY=<cadena> (obligatorio): clave de vinculación que recuperó de la instancia de Tenable Identity Exposure.
- EDIT_INSTANCENAME=<cadena> (opcional): nombre de la instancia de Relay. Si no define un nombre, Tenable Identity Exposure usa el nombre de la máquina. Puede modificar este nombre en Tenable Identity Exposure. Este nombre debe ser exclusivo.
- PROXY_ADDRESS=<IP o DNS> (opcional): dirección del proxy que se usará si la red requiere un servidor proxy para acceder a los dominios de Tenable. Si indica una dirección de proxy, también debe indicar un puerto de proxy.
- PROXY_PORT=<número> (opcional): puerto del proxy que se usará si la red requiere un servidor proxy para acceder a los dominios de Tenable. Si indica una dirección



de proxy, también debe indicar un puerto de proxy.

- /L* <carpeta> (opcional): ruta donde la instalación crea un archivo que contiene solo los registros de instalación de Relay.

Ejemplo de instalación de Secure Relay con opciones

```
.\tenable.ad_SecureRelay_v3.43.0.exe /qn APPDIR=D:\Tenable\Tenable.ad\ EDIT_LINKINGKEY=eyJjZXRpRG5zIjoicWExc2Fhcy1yZWxheS50ZW5hYmx1LmFkIiwidG9rZW4iOiI4NkYwMzMzQS01MkI5LTQ0QTctQjMxMS05RDdGRkM5QjkzNTUifQ== EDIT_INSTANCENAME="US Network Area" /L* C:\Users\Administrator\Desktop\log.txt
```

Nota: Al presionar Intro, la instalación comienza como tarea en segundo plano. Aunque el aviso de la CLI aparezca de inmediato, no es indicativo de que la instalación se haya completado. Si seleccionó la opción /L*, puede consultar el archivo de registros para confirmar que la instalación se haya completado correctamente.

Ejemplos

Los siguientes son ejemplos de entradas de registros que indican instalaciones correctas o con errores:

Instalación correcta

```
MSI (s) (D8:EC) [17:39:04:383]: Product: Tenable.ad Secure Relay -- Installation completed successfully.
```

```
MSI (s) (D8:EC) [17:39:04:383]: Windows Installer installed the product. Product Name: Tenable.ad Secure Relay. Product Version: 3.43.0. Product Language: 1033. Manufacturer: Tenable. Installation success or error status: 0.
```

```
=== Logging stopped: 3/15/2023 17:39:04 ===
```

Instalación con errores

```
MSI (s) (74:38) [17:18:35:713]: Product: Tenable.ad Secure Relay -- Installation failed.
```

```
MSI (s) (74:38) [17:18:35:713]: Windows Installer installed the product. Product Name: Tenable.ad Secure Relay. Product Version: 3.43.0. Product Language: 1033. Manufacturer: Tenable. Installation success or error status: 1603.
```

```
=== Logging stopped: 3/15/2023 17:18:35 ===
```

Instalar Secure Relay (Agente de Tenable Nessus)



En el siguiente procedimiento se instala Secure Relay mediante el Agente de Tenable Nessus.

Antes de empezar

- Compruebe haber [descargado](#) e [instalado](#) el Agente de Tenable Nessus.

Nota: El programa de instalación del Agente de Tenable Nessus solicita una clave de agente. Esta clave **no es obligatoria** para la funcionalidad Secure Relay.

- Cumpla con los requisitos previos necesarios y obtenga la **clave de vinculación obligatoria**, como se describe en [Secure Relay](#).

Para instalar Secure Relay mediante Nessus:

1. En una máquina que hospeda el Agente de Tenable Nessus y actúa como Relay, abra una ventana del símbolo del sistema de administrador en el directorio del Agente de Tenable Nessus (C:\Archivos de programa\Tenable\Nessus Agent) y escriba el siguiente comando:

Instalación de Secure Relay

```
nessuscli install-relay --linking-key=<Relay Linking Key> --proxy-host=<Customer Proxy IP or DNS> --proxy-port=<Customer Proxy Port>
```

2. Reemplace <Tenable Identity Exposure Relay Linking Key> por el valor que copió anteriormente de la instancia de Tenable Identity Exposure e indique una dirección y un número de puerto de proxy si usa un servidor proxy.

Comienza la instalación. Se necesitan unos minutos para ejecutar las verificaciones de conectividad y el proceso de instalación.

Cuando la instalación se completa correctamente, aparece un mensaje para indicar que Relay se está ejecutando en la máquina host.



```
Administrator: Command Prompt

Backup Tool:
  backup --create <backup file filename>
  backup --restore <backup file path>

Tenable.AD Integration:
  install-relay --linking-key=<Tenable.AD Relay Linking Key>

Image Preparation Commands:
  prepare-image [--json=<file>]

C:\Program Files\Tenable\Nessus Agent>nessuscli install-relay --linking-key=eyJjZXRpRG5zIjoicWExc2Fhcy1yZWxheS50ZW5hYmx1
LmFkIiwidG9rZW4iOiI1NDZDMTM4RS1BODAyLTQzNjktQjY4RC1FNjE4ODFCMDlGMzQifQ==

Initiating install of Tenable.AD Secure Relay

Testing connectivity to qa1saas-relay.tenable.ad with relay name da3b8709-e47c-47b5-bd08-216ddf8e471f
Connectivity test passed.

Downloading install package from https://qa1saas-relay.tenable.ad/auto-update/latest

Installing C:\ProgramData\Tenable\Nessus Agent\nessus\tmp\tenable.ad_SecureRelay_v9.9.11.exe

Checking if the relay is running: yes
The Tenable.AD Secure Relay successfully installed on this host.

C:\Program Files\Tenable\Nessus Agent>
```

3. En Tenable Identity Exposure, haga clic en **Sistema > Gestión de Relay**. La instancia de Relay recién instalada aparece en la lista de instancias de Relay con el identificador que se muestra en la ventana de instalación.



Solucionar problemas de instalación de Secure Relay

Eliminación del archivo de configuración mediante EDR o antivirus durante la instalación

- **Causa:** durante la instalación de Secure Relay, el software de detección y respuesta de puntos de conexión (EDR) o los programas antivirus pueden interferir con el proceso al eliminar



automáticamente el archivo de configuración `envoy.yaml`. Este archivo es fundamental para que Secure Relay funcione correctamente. Si se elimina, la instalación falla.

- **Mensaje de error:** si sospecha que el error en la instalación se debe a que el software EDR o antivirus eliminaron el archivo `envoy.yaml`, puede consultar el registro de errores de MSI para confirmarlo. El registro de errores de MSI se genera en la carpeta TEMP del sistema. Busque el siguiente mensaje de error: `Error: The file envoy.yaml is missing`(Error: Falta el archivo `envoy.yaml`).

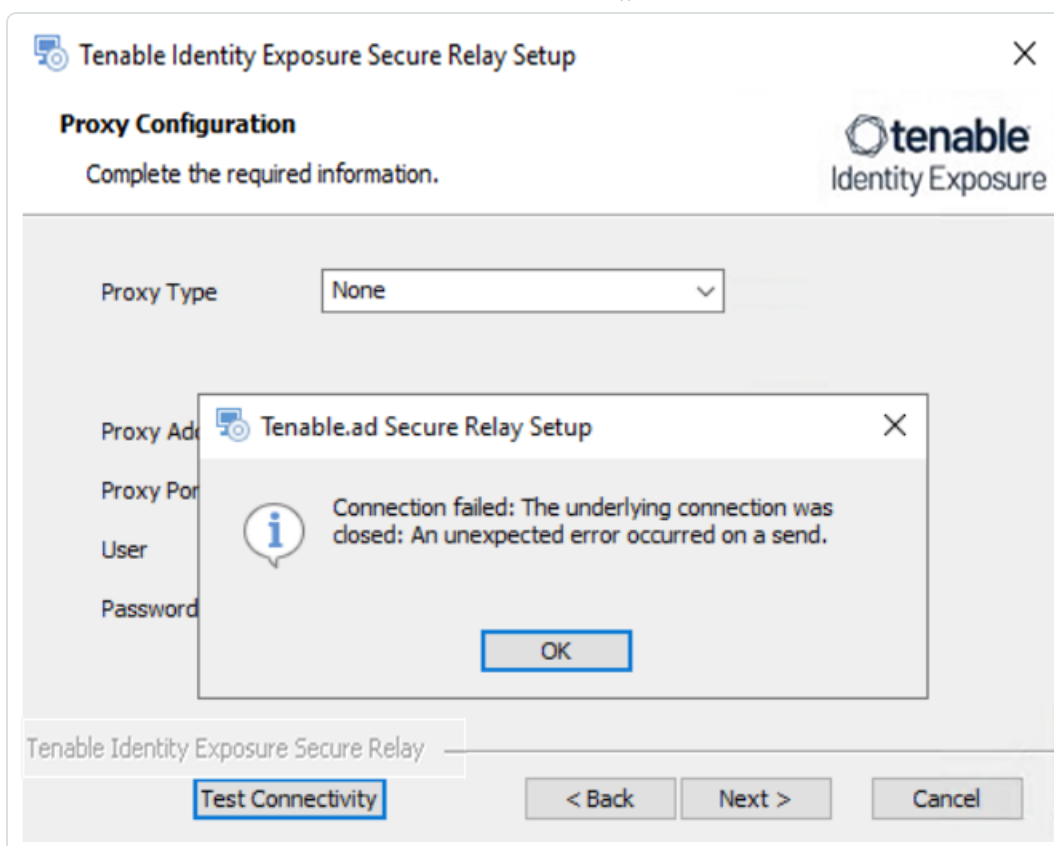
Si este error aparece en el registro, indica que, probablemente, un software de seguridad eliminó el archivo `envoy.yaml` durante el proceso de instalación.

- **Solución:** para resolver este problema y garantizar una instalación correcta, siga los pasos a continuación:

1. Permita la carpeta de instalación o el archivo de configuración:
 - Configure el software EDR o antivirus para excluir el siguiente directorio de los escaneos y acciones de eliminación: `[ruta_de_instalación]\Tenable.ad\SecureRelay\`
 - Como alternativa, puede incluir en la whitelist el archivo `[ruta_de_instalación]\Tenable.ad\SecureRelay\envoy.yaml` si no puede excluir la carpeta entera.
2. Reintentar la instalación: después de agregar las exclusiones necesarias, vuelva a ejecutar la instalación de Secure Relay.

Error de instalación de varias instancias de Secure Relay y una instancia de Secure Relay en un servidor independiente

- **Causa:** durante la actualización, el instalador no detecta la variable de entorno para la dirección IP del host de Ceti y establece el valor predeterminado "127.0.0.1".
- **Mensaje de error:** Falló la conexión debido a un error inesperado durante la transmisión.



- **Solución:**

1. Verifique la variable de entorno "TENABLE_CASSIOPEIA_CETI_Service__Broker__Host" en el servidor de Directory Listener.
2. Asegúrese de que esté **definida en la dirección IP de Security Engine Node**. Si la variable está definida en el valor predeterminado "127.0.0.1", provoca que la instalación de Secure Relay falle.
3. Después de actualizar la variable de entorno "TENABLE_CASSIOPEIA_CETI_Service__Broker__Host", **reinicie el servicio Ceti**.
4. **Comience nuevamente la instalación de Secure Relay**. De lo contrario, se revierte y deja los servicios Relay y Envoy instalados y bloquea toda instalación futura.

Nombre de CetiDNS no válido

- **Causa:** la dirección IP del servidor de Ceti no se configuró durante la actualización o instalación del servidor de Security Engine Node. El instalador tiene como valor

predeterminado "127.0.0.1":

Tenable Identity Exposure Setup

Directory Listener
Complete the required fields.

Ceti

Host 127.0.0.1

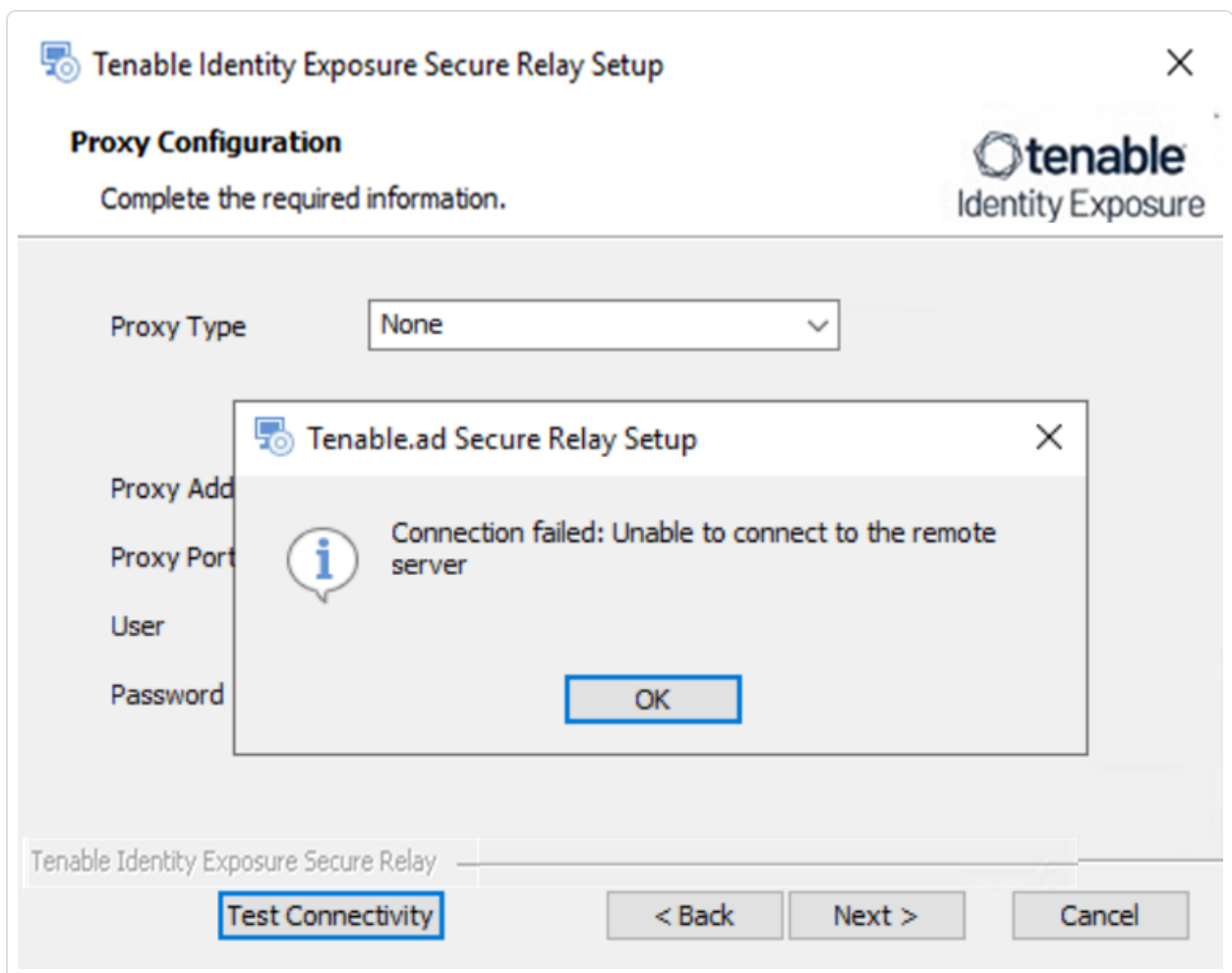
Yes (Installation will start automatically after the reboot)

No

Install a Secure Relay on this machine.

< Back Next > Cancel

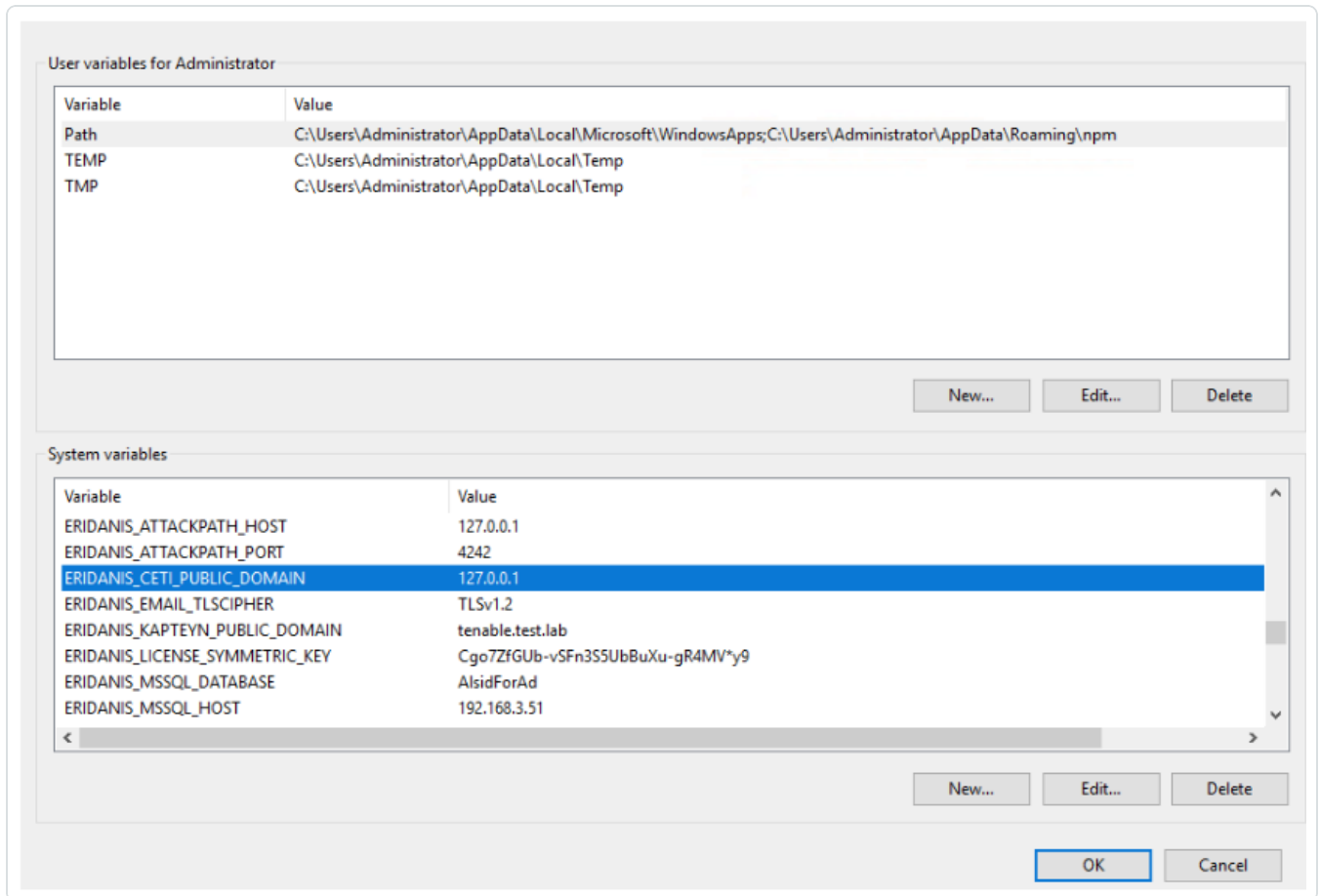
- **Mensaje de error:** Error de conexión: no se puede conectar al servidor remoto.



Para el servicio “tenable_envoy_server” en estado de pausa: identifique la aplicación que actualmente ocupa el puerto 0.0.0.0:443 mediante el comando de PowerShell `netstat -anob | findstr 443`. Si encuentra otra aplicación, quítela o deténgala para resolver el conflicto y permitir el correcto funcionamiento del servicio “tenable_envoy_server”.

Solución:

1. Inicie sesión en el servidor de Security Engine Node.
 - Si utiliza una arquitectura dividida de Security Engine Node, inicie sesión en el servidor que ejecuta el servicio Eridanis.
2. Abra “Variables de entorno” y busque el nombre de variable ERIDANIS_CETI_PUBLIC_DOMAIN.

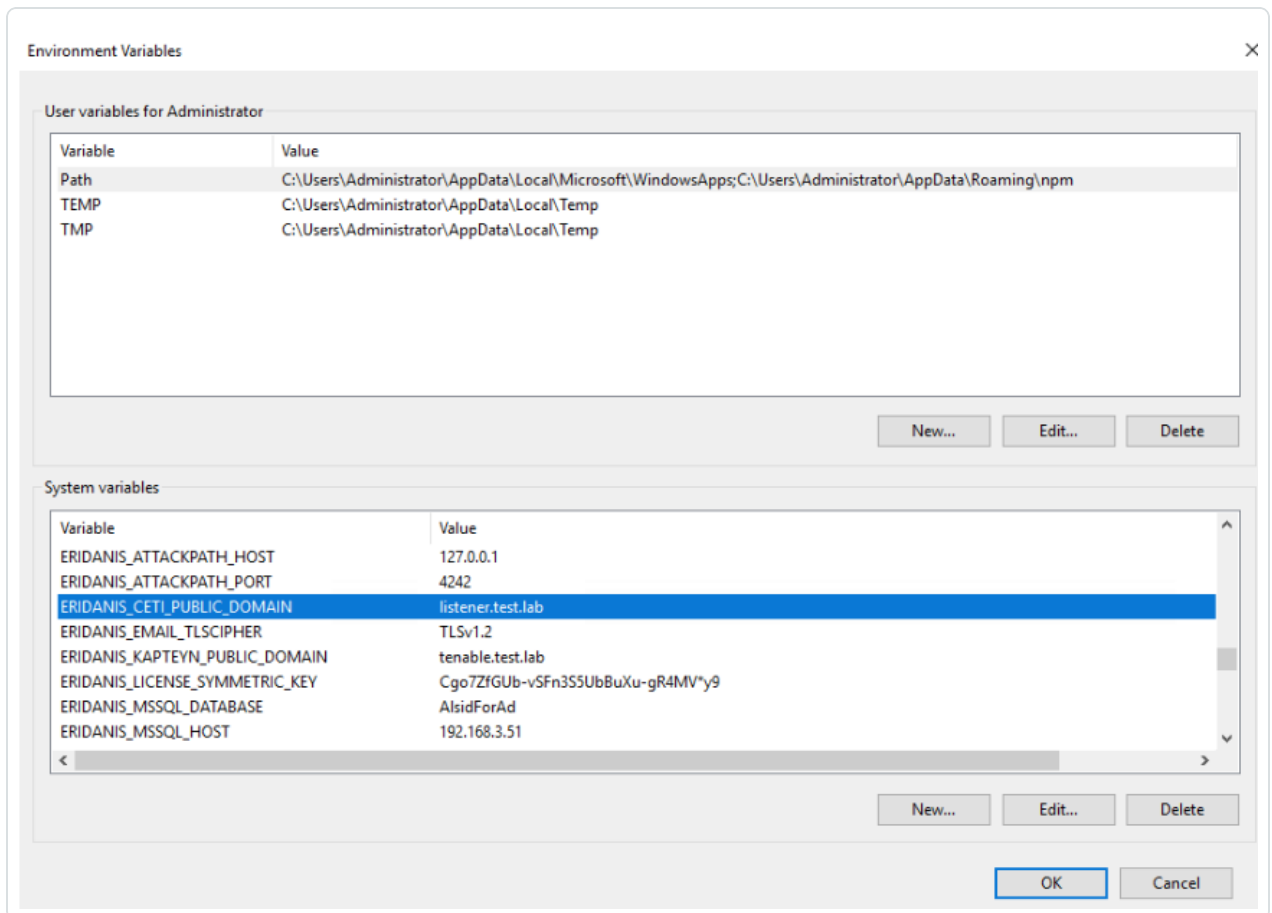


3. Edite el valor de la variable ERIDANIS_CETI_PUBLIC_DOMAIN para insertar la **dirección IP o el nombre de host de Directory Listener**:

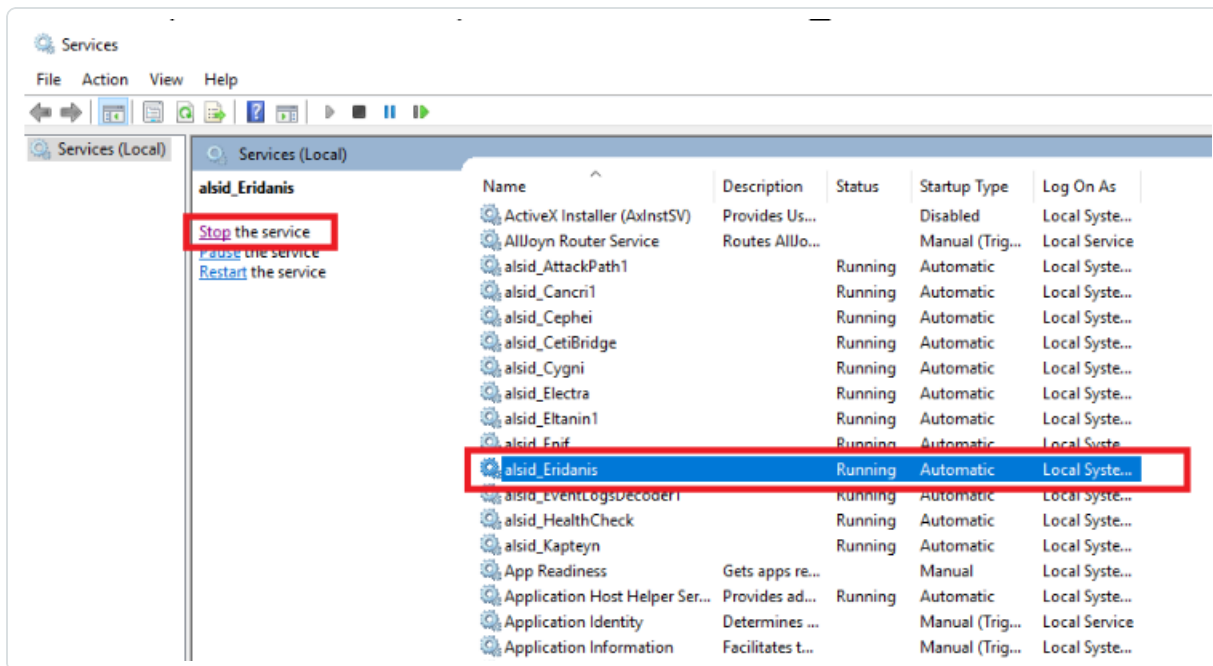
- Actualice la variable de entorno ERIDANIS_CETI_PUBLIC_DOMAIN para que coincida con la dirección IP o el nombre de host de Directory Listener. Esta sincronización facilita la comunicación fluida entre los componentes implementados en servidores independientes.
- El valor de la variable "ERIDANIS_CETI_PUBLIC_DOMAIN" cambia de 127.0.0.1 a la



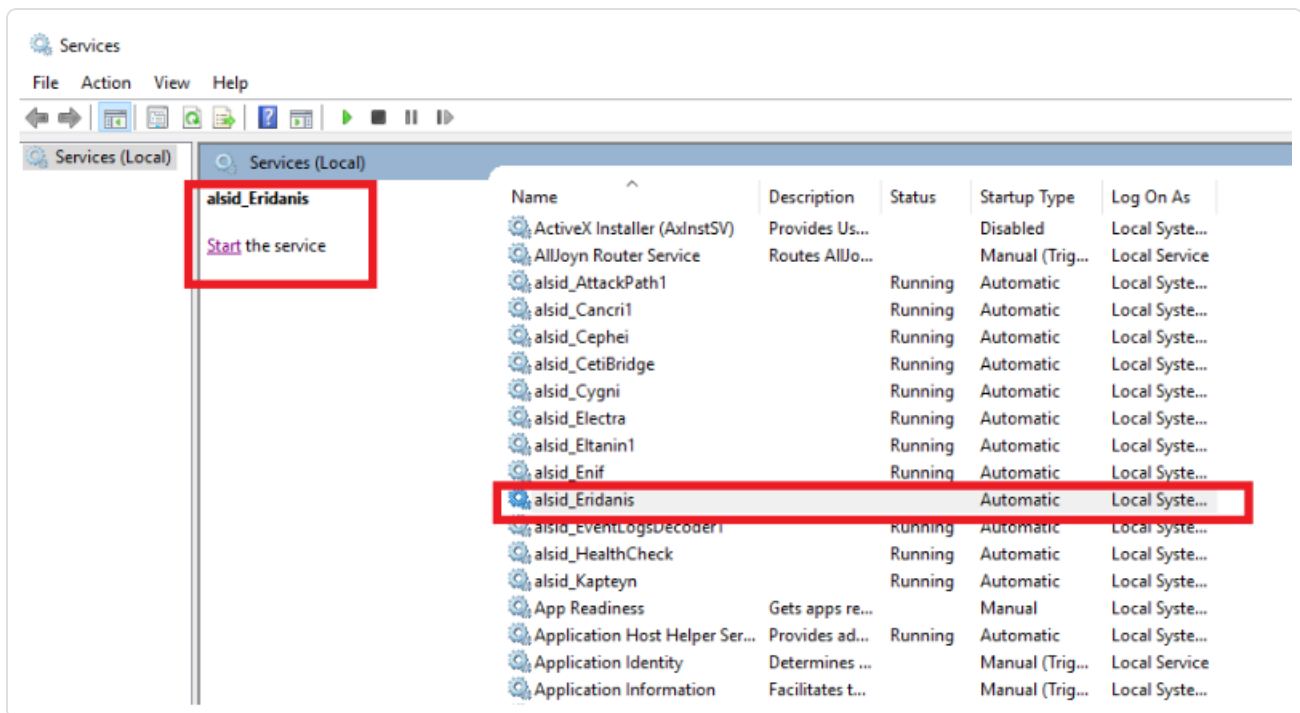
dirección IP o el nombre de host de Directory Listener `listener.test.lab`.



4. Abra "Servicios" y detenga el servicio tenable_Eridanis.



5. Inicie el servicio tenable_Eridanis.



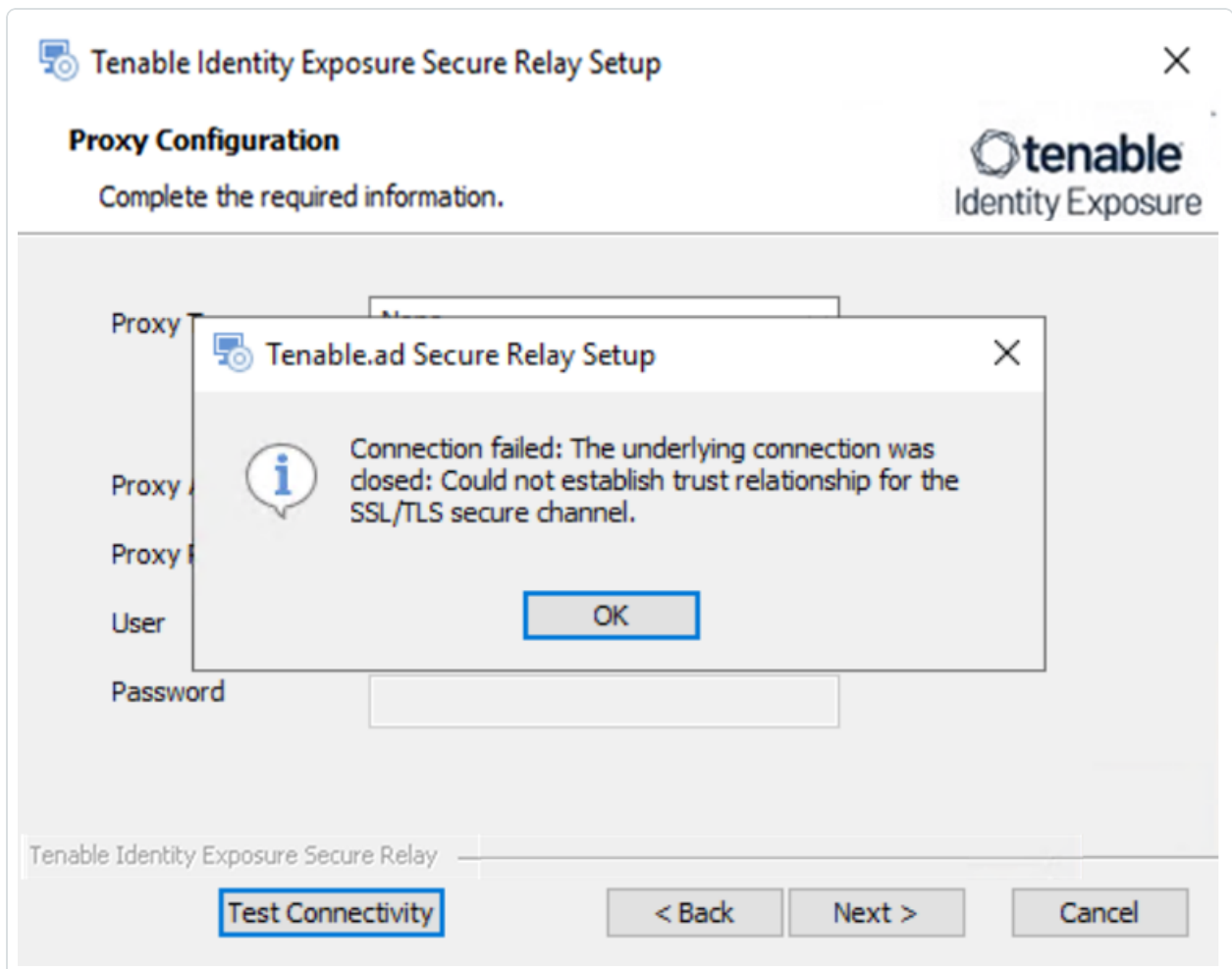


6. Inicie sesión en el servidor de Secure Relay. Salga del instalador de Secure Relay si ya está abierto y vuelva a comenzar la instalación de Secure Relay.

Precaución: Asegúrese de **salir del instalador** y comenzar una nueva instalación. Si no sale del instalador y continúa con la instalación, el proceso de instalación se interrumpe y no se puede continuar (bloqueador).

No existe una "relación de confianza" para la conexión segura SSL/TLS

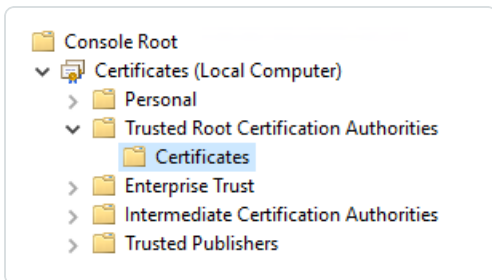
- **Causa:** el instalador no puede encontrar los certificados de entidad de certificación en el servidor local.
- **Mensaje de error:** Error de conexión: la conexión subyacente se cerró: no se pudo establecer una relación de confianza para el canal seguro SSL/TLS.



- **Solución:**



1. Acceda al sistema de origen (servidor de Directory Listener) o al repositorio donde residen los certificados de CA de confianza y busque dichos certificados, en general en directorios como:
 - Ubicación predeterminada de los certificados autofirmados: “unidad_de_instalación”:\Tenable\Tenable.ad\DefaultPKI\Certificates\ca
 - Ubicación personalizada de los certificados: “unidad_de_instalación”:\Tenable\Tenable.ad\Certificates\
2. Copie los archivos de certificados de entidad de certificación de confianza del sistema de origen (servidor de Directory Listener) en el servidor local (servidor de Secure Relay).
3. Importe los certificados al almacén de certificados de confianza del servidor de Secure Relay.



4. Después de una importación correcta, **salga del instalador de Secure Relay y vuelva a comenzar la instalación.**

Precaución: Asegúrese de **salir del instalador** y comenzar una nueva instalación. Si no sale del instalador y continúa con la instalación, el proceso de instalación se interrumpe y no se puede continuar (bloqueador).



Comenzar a usar Tenable Identity Exposure

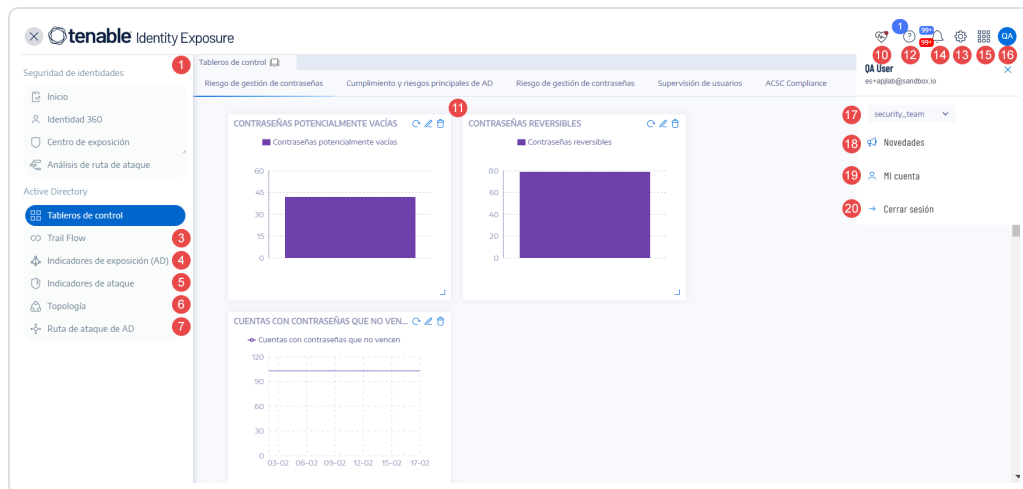
Después de implementar Tenable Identity Exposure, esta sección le guiará por los pasos clave para comenzar a usar Tenable Identity Exposure de manera eficaz.

Cada sección contiene vínculos a descripciones e instrucciones más detalladas para la tarea relacionada.



1. Iniciar sesión y navegar por la interfaz de usuario

- [Iniciar sesión en Tenable Identity Exposure](#) portal. Se abre la página de inicio, como se muestra en este ejemplo.
- Su nombre de usuario inicial es `hello@tenable.ad` y la contraseña es `Hello@tenable.ad123!`.
- Expanda o contraiga la barra de navegación lateral:
 - Para expandirla, haga clic en el menú  en la parte superior izquierda de la ventana.
 - Para contraerla, haga clic en  en la parte superior izquierda de la ventana.



- Navegue por el [Portal del usuario de Tenable Identity Exposure](#).

2. Instalar Secure Relay

Secure Relay transfiere de forma segura datos de Active Directory desde su red a la plataforma de Tenable Identity Exposure SaaS mediante el cifrado TLS en lugar de una conexión VPN. Es posible utilizar varias instancias de Secure Relay en función de sus requisitos.

Requisitos previos:



- Acceso administrativo a una instancia de Windows Server para la máquina virtual (VM) de Secure Relay.
- Instalador más reciente de Secure Relay descargado del portal de descargas de Tenable Identity Exposure.
- Una clave de vinculación de un solo uso del portal de Tenable Identity Exposure, que contiene la dirección de red y el token de autenticación.

Para conocer los requisitos previos detallados, consulte [Secure Relay de Tenable Identity Exposure](#).

Recuperar la clave de vinculación:

1. Conéctese al portal web de Tenable Identity Exposure con una cuenta de administrador.
2. Haga clic en **Sistema > Configuración > pestaña Relay**.
3. Haga clic en el ícono **Copiar en el portapapeles** junto a la clave de vinculación.

Instalar Secure Relay:

1. En la VM de Windows Server, haga clic con el botón derecho en el archivo de instalación y seleccione **Ejecutar como administrador**.
2. En el asistente de instalación, haga clic en **Siguiente** en la pantalla de bienvenida.
3. En la ventana **Configuración personalizada**, haga clic en **Explorar** para cambiar la partición del disco si es necesario y, luego, haga clic en **Siguiente**.
4. En la ventana **Clave de vinculación**:
 - Pegue la clave de vinculación que copió del portal.
 - Escriba un nombre para la instancia de Secure Relay.
 - Haga clic en **Probar la conectividad**.
5. Si la prueba es correcta (ícono verde), haga clic en **Siguiente**. En caso contrario, haga clic en **Volver** para corregir los errores.



6. En la ventana **Listo para instalar**, haga clic en **Instalar**.
7. Una vez que se instale, haga clic en **Finalizar**.

Para conocer el procedimiento detallado, consulte [Secure Relay de Tenable Identity Exposure](#).

Verificar la instalación de Relay en el portal:

1. Regrese al portal de Tenable Identity Exposure.
2. Haga clic en **Sistema** > pestaña **Gestión de Relay**.

La instancia de Relay recién instalada aparece en la lista Relay.

Configurar Relay:

Cuando agrega dominios para supervisar, aparece una nueva opción que le permite seleccionar la instancia de Secure Relay a cargo de ese dominio. Consulte [Configurar Relay](#) para conocer el procedimiento completo.

Actualizaciones automatizadas:

De forma periódica, Tenable Identity Exposure comprueba si hay actualizaciones de Secure Relay y las instala automáticamente (requiere acceso HTTPS). Un ícono en la bandeja de red indica cuándo tienen lugar las actualizaciones. Después de la actualización, los servicios de Tenable Identity Exposure se reinician y se reanuda la recopilación de datos.

3. **Habilitar indicadores de exposición (IoE) para un dominio de Active Directory**

Antes de configurar los indicadores de exposición, debe tener una cuenta de servicio de Active Directory, o crear una, con los permisos adecuados. Si bien Tenable Identity Exposure no requiere privilegios de administrador para la supervisión de la seguridad, algunos contenedores requieren una configuración manual para permitir el acceso de lectura al usuario de la cuenta de servicio.

Para obtener información completa, consulte [Acceder a objetos o contenedores de AD](#).



1. Inicie sesión en el portal web de Tenable Identity Exposure con credenciales administrativas, como la cuenta predeterminada "hello@tenable.ad".
2. Haga clic en el ícono de menú en la parte superior izquierda para expandir el panel de navegación y, luego, haga clic en **Sistema** en el panel izquierdo.

Agregar un bosque:

1. En la pestaña **Gestión de bosques**, haga clic en **Agregar un bosque**.
2. Indique un nombre para mostrar para el bosque (por ejemplo, Tenable).
3. Escriba el nombre de usuario y la contraseña de la cuenta de servicio que va a conectarse a todos los dominios de este bosque.
4. Haga clic en **Agregar**.

Para obtener detalles completos, consulte [Bosques](#).

Agregar un dominio:

1. Haga clic en **Agregar un dominio**.
2. Indique un nombre para mostrar para el dominio que va a supervisar (por ejemplo, HQ).
3. Escriba el nombre de dominio completo (por ejemplo, sky.net).
4. De la lista desplegable, seleccione el bosque correspondiente.
5. Si usa SaaS con Secure Relay, seleccione la instancia de Relay para manejar este dominio.
6. Habilite el conmutador "[Análisis con privilegios](#)" si la cuenta tiene los privilegios necesarios.
7. Si habilita **Análisis con privilegios**, tiene la opción de habilitar **Transferencia de análisis con privilegios** para Tenable Cloud.
8. Proporcione detalles para el controlador de dominio con el rol FSMO del emulador del controlador de dominio principal:



- Dirección IP o nombre de host.
 - Deje los puertos LDAP, Catálogo global y SMB con los valores predeterminados ya rellenados.
9. Haga clic en **Probar la conectividad** al final.
 10. Si es correcto, haga clic en **Agregar**.

En la vista "Gestión de dominios", verá columnas para los estados de inicialización de LDAP, inicialización de SISFull y configuración de cuenta honey con un ícono de carga circular hasta que se complete el rastreo inicial.

Para obtener detalles completos, consulte [Dominios](#).

Inicialización del monitor:

1. Cambie a la vista **Trail Flow**. Después de unos minutos, los datos comienzan a moverse una vez que se inicia el análisis.
2. Regrese a **Sistema > Gestión de dominios**.
3. Espere a que aparezcan los íconos verdes que indican que se completó la inicialización de LDAP y SYSVOL.

Ahora tiene habilitada la supervisión de indicadores de exposición para este dominio. Las notificaciones en el portal web aparecen en minutos u horas, según el tamaño del entorno.

Revisar los datos de exposición:

1. Haga clic en **Indicadores de exposición** en el menú izquierdo para ver todos los indicadores desencadenados para el dominio agregado.
2. Haga clic en un indicador para ver los detalles del objeto anómalo que provocan la falta de conformidad.
3. Cierre los detalles y vaya a **Tableros de control** para ver las métricas del entorno.

4. Implementar indicadores de ataque (IoA) para un dominio



Para implementar loA, primero debe encargarse de tres configuraciones según se describe a continuación:

1. El script de loA es obligatorio para todos los escenarios de ataque.
2. La cuenta honey se debe configurar para detectar ataques específicos, como Kerberoasting.
3. Instalación de Sysmon en todos los controladores de dominio del dominio supervisado para detectar ataques, como el volcado de credenciales del sistema operativo.

Tenable Identity Exposure proporciona el script de loA, su línea de comandos y la línea de comandos de configuración de la cuenta honey. Sin embargo, debe cumplir estos requisitos previos directamente en los controladores de dominio o en una máquina administrativa con los derechos adecuados.

Para obtener información completa, consulte [Implementación de indicadores de ataque](#).

Configurar los escenarios de ataque:

1. Inicie sesión en el portal web de Tenable Identity Exposure con credenciales administrativas (por ejemplo, hello@tenable.ad).
2. Vaya a **Sistema > Configuración > Indicadores de ataque**.
3. Seleccione los escenarios de ataque que quiere habilitar para el entorno.
4. Seleccione la casilla debajo del nombre de dominio para habilitar todos los escenarios de ataque disponibles.
5. Haga clic en **Guardar** en la parte inferior derecha.
6. Haga clic en **Ver el procedimiento** al principio.
Aparece una ventana en la que se muestra el procedimiento para implementar el motor de loA.
7. Utilice el conmutador para habilitar o deshabilitar la funcionalidad de actualizaciones automáticas.



8. Haga clic en el primer botón **Descargar** para descargar el archivo PS1.
9. Haga clic en el segundo botón **Descargar** para descargar el archivo JSON.
10. Anote la ubicación donde descargó los archivos de instalación.
11. Busque el campo denominado **Ejecute los siguientes comandos de PowerShell**.
12. Copie el contenido del campo de texto y péguelo en un archivo de texto.
13. Copie los archivos PS1 y JSON en un controlador de dominio o en un servidor administrativo con los derechos adecuados.
14. Inicie el módulo de Active Directory para Windows PowerShell como administrador y navegue hasta la carpeta que aloja los archivos.
15. Pegue el comando que copió del portal web de Tenable Identity Exposure y presione Intro.
16. Abra la Consola de administración de directivas de grupo y busque el GPO denominado "Tenable.ad" vinculado a la unidad organizativa del controlador de dominio.

Para conocer el procedimiento detallado, consulte [Instalar indicadores de ataque](#).

Configurar la cuenta honey:

1. Regrese al portal web de Tenable Identity Exposure.
2. Vaya a **Sistema** > pestaña **Gestión de dominios**.
3. Haga clic en el ícono **+** debajo de **Estado de configuración de la cuenta honey** a la derecha de su dominio (disponible una vez que los otros dos estados estén en verde).
4. En el cuadro de búsqueda **Nombre**, escriba el nombre de la cuenta que quiere usar como sistema trampa.
5. Seleccione de la lista desplegable el nombre distintivo del objeto.
6. Copie el contenido del campo de texto de la línea de comandos y péguelo en un archivo de texto.
7. Regrese al servidor donde ejecutó el script de IoA.



8. Abra o inicie una línea de comandos de PowerShell como administrador.
9. Pegue el comando que copió del portal web de Tenable Identity Exposure y presione Intro.
10. Confirme que la línea de comandos se haya ejecutado correctamente.
11. Regrese al portal web de Tenable Identity Exposure y haga clic en el botón **Agregar** al final.

Después de unos segundos, el estado de configuración de la cuenta honey debería mostrar un punto verde.

Para conocer el procedimiento detallado, consulte [Cuentas honey](#).

Instalar Sysmon:

El portal web de Tenable Identity Exposure no proporciona la implementación automática para Sysmon. Consulte [Instalar Microsoft Sysmon](#) para obtener el archivo de configuración de Sysmon necesario. Puede instalar Sysmon manualmente como se muestra en la documentación o mediante un GPO.

Para conocer el procedimiento detallado, consulte [Instalar Microsoft Sysmon](#).

5. **Configurar Microsoft Entra ID para Tenable Identity Exposure:**

Tenable Identity Exposure también admite Microsoft Entra ID junto con Active Directory con loE específicos para identidades de Entra ID.

Para obtener información completa, consulte [Compatibilidad con Microsoft Entra ID](#).

Crear la aplicación de Entra ID:

1. Inicie sesión en el portal de administración de Azure, en portal.azure.com, con las credenciales adecuadas.



2. Haga clic en el mosaico **Azure Active Directory** y luego en **Registros de aplicaciones** en el menú de la izquierda.
3. Haga clic en **Nuevo registro** y proporcione un nombre de aplicación (por ejemplo, "Aplicación de exposición de identidad").
4. Haga clic en **Registrarse** al final.
5. En la página "Descripción general" de la aplicación, anote el "Id. de la aplicación (cliente)" y el "Id. del directorio (inquilino)".
6. Haga clic en **Certificados y secretos** en el menú de la izquierda.
7. Haga clic en **Nuevo secreto de cliente**, escriba una descripción y establezca el vencimiento según la política.
8. Haga clic en **Agregar** y guarde de forma segura el valor del secreto que se muestra.
9. Haga clic en **Permisos de API** y en **Agregar un permiso**.
10. Seleccione **Microsoft Graph** y luego **Permisos de aplicación**.
11. Agregue los permisos siguientes: `Audit Log.Read.All`, `Directory.Read.All`, `IdentityProvider.Read.All`, `Policy.Read.All`, `Reports.Read.All`, `RoleManagement.Read.All` y `UserAuthenticationMethod.Read.All`.
12. Haga clic en **Agregar permisos** y en **Conceder consentimiento del administrador**.

Configurar Tenable Vulnerability Management:

1. Conéctese al portal web de Tenable Vulnerability Management con la cuenta adecuada.
2. Haga clic en **Menú > Configuración > Credenciales**.
3. Haga clic en **Crear credencial** y seleccione el tipo **Microsoft Azure**.
4. Escriba un nombre y una descripción, pegue el Id. del inquilino, el Id. de la aplicación y el Secreto del cliente.
5. Haga clic en **Crear**.
6. Haga clic en **Menú > Configuración > Mi cuenta > Claves de API**.



7. Haga clic en **Generar**, revise la advertencia y haga clic en **Continuar**.
8. Copie los valores de Clave de acceso y Clave secreta.

Configurar Tenable Identity Exposure:

1. Conéctese con una cuenta de administrador global.
2. Haga clic en **Menú > Sistema > Configuración > Tenable Cloud**.
3. Habilite **Activar compatibilidad con Microsoft Entra ID**.
4. Ingrese la Clave de acceso y la Clave secreta que se generaron anteriormente.
5. Haga clic en la marca de verificación para enviar las claves de API correctamente.
6. Haga clic en la pestaña **Gestión de inquilinos** y en **Agregar un inquilino**.
7. Escriba un nombre para el inquilino de Azure AD.
8. Seleccione la credencial de Azure que se creó anteriormente.
9. Haga clic en **Agregar**.

Supervisar y revisar los hallazgos:

1. Tenable Identity Exposure escanea el inquilino. Para ver la hora del próximo escaneo, pase el cursor sobre **Estado del escaneo**.
2. Cuando el primer escaneo finaliza, aparece un ícono verde en la columna **Estado del escaneo**.
3. Haga clic en **Indicadores de exposición** en el menú de la izquierda.
4. Utilice las pestañas para filtrar entre los indicadores de AD y Azure AD.
5. Active **Mostrar todos los indicadores** para ver todos los indicadores disponibles.
6. Tres pestañas muestran los **Detalles del indicador**, los **Hallazgos del inquilino** y las **Recomendaciones**.
7. Revise los posibles riesgos de exposición y la guía para su corrección.



6. Configurar y usar loE en el entorno

Tenable Identity Exposure usa indicadores de exposición para medir la madurez de la seguridad de la instancia de Active Directory y para asignar niveles de gravedad al flujo de eventos que se supervisan y analizan.

Para obtener información completa sobre los loE, consulte [Indicadores de exposición](#).

Acceder a los loE:

1. Inicie sesión en Tenable Identity Exposure.
2. Haga clic en el ícono de la parte superior izquierda para expandir el panel.
3. Haga clic en **Indicadores de exposición** en el lado izquierdo para ver los loE.

En la vista predeterminada se muestran los elementos de configuración del entorno que son potencialmente vulnerables, clasificados por gravedad: crítica, alta, media y baja.

Ver todos los loE:

- Haga clic en el botón a la derecha de **Mostrar todos los indicadores**.
 - Puede ver todos los loE disponibles en la instancia de Tenable Identity Exposure. Un elemento que no muestre ningún dominio es un elemento en el que no tiene esa exposición.
 - A la derecha de **Mostrar todos los indicadores**, se puede ver **Dominio**. Si en el entorno tiene varios dominios, haga clic en él y seleccione los dominios que quiere ver.

Buscar loE:

- Haga clic en **Buscar un indicador** y escriba una palabra clave, como "contraseña".
Aparecen todos los loE relacionados con contraseñas.

Revisar los detalles del loE:



- Para ver información adicional sobre un indicador, haga clic en él.
 - La vista detallada comienza con un resumen ejecutivo de la exposición en particular.
 - Luego se enumeran los documentos relacionados y las herramientas de ataque conocidas que pueden exponer este elemento en particular.
- A la derecha, verá **Dominios afectados**.
 - Haga clic en la pestaña **Detalles de la vulnerabilidad** para leer la información adicional sobre las verificaciones llevadas a cabo para este IoE.
 - Haga clic en la pestaña **Objetos anómalos** para ver la lista de objetos y motivos que desencadenaron la exposición.
 - Si expande un objeto en la lista, podrá ver más detalles sobre qué causó la anomalía.

Crear consultas:

1. Para crear una consulta, haga clic en **Escriba una expresión** e ingrese una consulta booleana para un elemento. También puede hacer clic en el ícono de filtro a la izquierda para crear una consulta.
2. Establezca las fechas inicial y final, elija los dominios y, para buscar elementos ignorados, haga clic en el botón **Ignorar**.

Para conocer los procedimientos completos, consulte [Buscar objetos anómalos](#).

Ignorar/exportar objetos anómalos:

- Para ocultar objetos en la lista, puede ignorarlos.
 - Seleccione uno o más objetos y haga clic en **Seleccionar una acción** al final de la página.
 - Seleccione **Ignorar los objetos seleccionados** y haga clic en **Aceptar**.



- Elija la fecha hasta la cual quiere ignorar los objetos seleccionados.
- Puede dejar de ignorar los objetos de la misma manera, con la opción **Dejar de ignorar los objetos seleccionados**.
- Para exportar como archivo CSV la lista de todos los objetos anómalos de este indicador, haga clic en el botón **Exportar todo**.

Para conocer los procedimientos completos, consulte [Objetos anómalos](#).

Recomendaciones de corrección:

- Haga clic en la pestaña **Recomendaciones** para ver las recomendaciones sobre cómo corregir este indicador.

Consulte también [Corregir las anomalías de los indicadores de exposición](#) para conocer casos de uso de corrección.

7. Hacer un seguimiento de los cambios de configuración de AD mediante Trail Flow

Trail Flow muestra la supervisión y el análisis en tiempo real de los eventos que afectan sus infraestructuras de AD. Le permite detectar vulnerabilidades críticas y las acciones de corrección recomendadas.

Para obtener información completa, consulte [Trail Flow](#) y [Casos de uso de Trail Flow](#).

Acceder a Trail Flow:

1. Inicie sesión en Tenable Identity Exposure.
2. Haga clic en el ícono de la parte superior izquierda para expandir la barra de navegación.
3. Haga clic en **Trail Flow**.

Navegar por la página "Trail Flow":

La página "Trail Flow" se abre con una lista de eventos, incluido el tipo de origen, la ruta del objeto, el dominio y la fecha.



1. Haga clic en el cuadro de fecha en la parte superior derecha para indicar las fechas que está buscando.
2. Haga clic en **Dominio** para cambiar los servidores o bosques de Active Directory.
3. Haga clic en el botón de pausa en la esquina superior derecha para pausar o reiniciar la captura de Trail Flow.

Crear consultas:

Hay dos formas de crear consultas para una búsqueda: de forma manual o con el asistente.

- Para filtrar eventos de forma manual, escriba una expresión en el cuadro de búsqueda para acotar los resultados mediante los operadores booleanos.

Para obtener información completa, consulte [Buscar en Trail Flow de forma manual](#).

- Para utilizar el asistente de búsqueda:
 1. Haga clic en el ícono de la varita mágica a la izquierda.
 2. Siga las instrucciones para crear y combinar las expresiones de consulta.

Para obtener información completa, consulte [Buscar en Trail Flow con el asistente](#) y [Personalizar las consultas de Trail Flow](#).

Ver los detalles de un evento:

Una vez que haya detectado un evento importante:

1. Haga clic en el evento. Se mostrarán los atributos del cambio en ese objeto.
2. Pase el cursor por el ícono del punto azul a la izquierda para comparar los valores antes del evento y durante este.
3. Pase el cursor por los elementos para ver información adicional.
4. Haga clic en **Ver valor total** y haga clic en el botón para copiar esa información en el portapapeles.



Detectar cambios en la configuración:

Uno de los desafíos de ciberseguridad en los servidores de Active Directory es la gran cantidad de cambios de configuración que no afectan la exposición cibernética. Para detectar cambios en la configuración:

1. Haga clic en el ícono de la varita mágica.
2. Habilite **Solo anómalo**.
3. Haga clic en **Validar**.

Ver elementos de exposición cibernética:

Observe que los eventos tienen un símbolo de diamante rojo junto a ellos. Haga clic en un evento para ver la información sobre el cambio en la configuración. Hay una pestaña adicional disponible denominada "Anomalías". Haga clic en ella para ver los elementos de exposición cibernética específicos que se crearon o resolvieron.

8. Detectar mediante loA posibles ataques a AD

Los indicadores de ataque (loA) de Tenable Identity Exposure le brindan la capacidad de detectar ataques a su instancia de Active Directory (AD).

Para obtener información completa, consulte [Indicadores de ataque](#).

Acceder a los loA:

1. Inicie sesión en Tenable Identity Exposure.
2. Haga clic en el ícono de la parte superior izquierda para expandir la barra de navegación.
3. Haga clic en **Indicadores de ataque**.

Filtrar la línea temporal:

De manera predeterminada, verá la línea temporal de detección de ataques para el día de hoy. Para cambiar el filtro:



- Haga clic en **Día**, Mes o **Año**.
- Para cambiar el período de tiempo, haga clic en el ícono del calendario y seleccione el período de tiempo apropiado.

Filtrar la vista:

Puede filtrar la vista por dominios o loA específicos con el selector en el lado derecho del portal.

1. Haga clic en **Dominios** para ver y seleccionar las opciones.
2. Haga clic en la **X** para cerrar.
3. Haga clic en **Indicadores** para ver y seleccionar las opciones.
4. Haga clic en la **X** para cerrar.

A modo de ejemplo, vamos a centrarnos en lo que ocurrió en 2022:

1. Haga clic en el botón **Año** y seleccione "2022".
2. Haga clic en la barra roja y amarilla en la línea temporal.
3. Ahora puede consultar una nueva vista con los tres principales ataques críticos y los tres principales ataques de gravedad media detectados ese mes.
4. Para cerrar la vista, haga clic fuera del cuadro negro.

Ver los detalles de los ataques detectados:

Debajo de la línea temporal, verá una tarjeta para el dominio supervisado en el que se detectó el ataque.

- Haga clic en el menú desplegable **Ordenar por**.
- Puede ordenar la tarjeta por dominio, criticidad del indicador o bosque.
- Para buscar un dominio o ataque en particular, use el cuadro de búsqueda.



- De manera predeterminada, solo verá una tarjeta para el dominio bajo ataque. Para alternar la vista para ver cada dominio, cambie **Mostrar solo dominios bajo ataque** de **Sí** a **No**.

Personalizar el gráfico:

Una tarjeta contiene dos tipos de información: un gráfico y los tres ataques principales.

1. Para cambiar el tipo de gráfico, haga clic en el ícono de lápiz en la parte superior derecha de la tarjeta.
2. Seleccione **Distribución de ataques** o **Cantidad de eventos**.
3. Haga clic en **Guardar**.

Consultar los detalles de un incidente:

Para ver más detalles sobre el ataque que se detectó:

- Haga clic en la tarjeta para ver los incidentes relacionados con el dominio.
- Para filtrar, utilice el cuadro de búsqueda, seleccione una fecha inicial o final, elija indicadores específicos o alterne la casilla **No/Sí** para mostrar u ocultar los incidentes cerrados.
- Para cerrar incidentes, seleccione una alerta, haga clic en el menú **Seleccionar una acción** al final, seleccione **Cerrar incidentes seleccionados** y haga clic en **Aceptar**.
- Para reabrir un incidente, seleccione una alerta, haga clic en el menú **Seleccionar una acción**, seleccione **Reabrir incidentes seleccionados** y haga clic en **Aceptar**.

Ver los detalles de un ataque y las reglas de detección YARA:

- Haga clic en un ataque para abrir la vista detallada. En el panel de descripción, encontrará la descripción del incidente del ataque, información del marco MITRE ATT&CK y recursos adicionales con vínculos a sitios web externos.
- Haga clic en el panel de reglas de detección YARA para ver un ejemplo de una regla que pueda realizar una investigación de malware en las herramientas de detección.



- Para exportar la lista de incidentes, haga clic en **Exportar todo**. El único formato disponible es CSV.

Notificaciones y alertas:

El ícono de la campana en la parte superior derecha muestra una notificación cuando Tenable Identity Exposure detecta un ataque. Estos ataques aparecen en la pestaña de alertas de ataques.

9.

Configurar y usar alertas

El sistema de alertas de Tenable Identity Exposure le ayuda a detectar regresiones de seguridad o ataques en su instancia de Active Directory supervisada. Envía datos de análisis sobre vulnerabilidades y ataques en tiempo real a través de notificaciones por correo electrónico o SYSLOG.

Para conocer los procedimientos completos, consulte [Alertas](#).

Configurar el servidor SMTP:

1. Conéctese a Tenable Identity Exposure.
2. Haga clic en **Sistema > Configuración**.
3. Configure el servidor SMTP desde este menú.

Crear alertas de correo electrónico:

1. En **Motor de alertas**, haga clic en **Correo electrónico**.
2. Haga clic en el botón **Agregar una alerta de correo electrónico**.
3. En el cuadro **Dirección de correo electrónico**, escriba la dirección de correo electrónico del destinatario.
4. En el cuadro **Descripción**, escriba una descripción para la dirección.



5. En la lista desplegable **Desencadenar la alerta**, seleccione **Si hay cambios, Con cada anomalía** o **Con cada ataque**.
6. En el menú desplegable **Perfiles**, seleccione los perfiles que quiere usar para esta alerta de correo electrónico.
7. Marque la casilla **Enviar alertas cuando se detecten anomalías** para enviar notificaciones por correo electrónico cuando un reinicio del sistema desencadene alertas.
8. En el menú desplegable **Umbral de gravedad**, seleccione el umbral al que Tenable Identity Exposure enviará alertas.
9. Seleccione los indicadores para los cuales quiere enviar alertas.
10. Seleccione los dominios para enviar alertas:
 - a. Haga clic en **Dominios** para seleccionar los dominios para los que Tenable Identity Exposure envía alertas.
 - b. Seleccione el bosque o dominio y haga clic en el botón **Filtrar selección**.
11. Haga clic en el botón **Probar la configuración**.

Un mensaje confirma que Tenable Identity Exposure envió una alerta de correo electrónico al servidor.
12. Haga clic en el botón **Agregar**.

Un mensaje confirma que Tenable Identity Exposure creó la alerta de correo electrónico.

Crear alertas de SYSLOG:

1. Haga clic en **SYSLOG** y luego haga clic en el botón **Agregar alerta de SYSLOG**.
2. En el cuadro **Dirección IP o nombre de host del recopilador**, escriba la dirección IP o el nombre de host del servidor que recibe las notificaciones.
3. En el cuadro **Puerto**, escriba el número de puerto del recopilador.
4. En el menú desplegable **Protocolo**, seleccione UDP o TCP.



5. Si elige TCP, seleccione la casilla de la opción **TLS** para habilitar el protocolo de seguridad TLS.
6. En el cuadro **Descripción**, escriba una descripción breve del recopilador.
7. Elija una de las tres opciones para activar alertas: **Si hay cambios**, **Con cada anomalía** o **Con cada ataque**.
8. En el menú desplegable **Perfiles**, seleccione los perfiles que quiere usar para esta alerta de SYSLOG.
9. Si quiere enviar alertas después de reiniciar o actualizar el sistema, marque **Enviar alertas cuando se detecten anomalías durante la fase de análisis inicial**.
10. Si configura las alertas para que se desencadenen cuando se produzcan cambios, escriba una expresión para desencadenar la notificación del evento.
11. Haga clic en el botón **Probar la configuración**.

Un mensaje confirma que Tenable Identity Exposure envió una alerta de SYSLOG al servidor.

12. Haga clic en **Agregar**.

Un mensaje confirma que Tenable Identity Exposure creó la alerta de SYSLOG.

10. **Configurar tableros de control en el portal de Tenable Identity Exposure**

Los tableros de control le permiten visualizar datos y tendencias que afectan la seguridad de su instancia de Active Directory. Puede personalizar los tableros de control con widgets para mostrar gráficos y contadores según sus requisitos.

Para obtener información completa, consulte [Tableros de control](#).

Acceder a los tableros de control:

1. Inicie sesión en Tenable Identity Exposure.
2. Haga clic en el ícono de la parte superior izquierda para expandir la barra de navegación.



Crear un tablero de control personalizado:

1. Vaya a **Tableros de control** y haga clic en **Agregar**.
2. Haga clic en **Agregar un tablero de control**.
3. Asígnele un nombre y haga clic en **Aceptar**.

Agregar widgets al tablero de control:

1. Haga clic en **Agregar** en la esquina superior derecha.
2. Seleccione **Agregar un widget a este tablero de control** o haga clic en el botón en el medio de la pantalla.
3. Elija el tipo de widget (gráficos de barras, gráficos de líneas o contadores).

Configurar un widget de gráfico de líneas:

1. Haga clic en **Gráficos de líneas**.
2. Asigne un nombre al widget; por ejemplo, "Anomalías de los últimos 30 días".
3. Seleccione el tipo de datos (conteo de usuarios, conteo de anomalías o puntuación de cumplimiento).
4. Seleccione **Anomalías** y configúrelo para un mes.
5. Haga clic en **No hay indicadores** y seleccione qué indicadores va a usar.
6. Asigne un nombre al conjunto de datos; por ejemplo, "Crítico".
7. Agregue otros conjuntos de datos según sea necesario (por ejemplo, para medio y bajo).
8. Haga clic en **Agregar**.

Agregar un widget de gráfico de barras:



1. Haga clic en **Gráfico de barras**.
2. Asígnele el nombre **Cumplimiento** y elija el tipo de datos de puntuación de cumplimiento.
3. Seleccione todos los indicadores.
4. Asigne un nombre al conjunto de datos; por ejemplo, "IoE".
5. Haga clic en **Agregar**.

Agregar un widget de contador:

1. Haga clic en **Contador**.
2. Asigne un nombre al widget (por ejemplo, "Usuarios") y establezca el tipo de datos en **Conteo de usuarios**.
3. Elija el estado **Todos** y seleccione el dominio.
4. Asigne un nombre al conjunto de datos y haga clic en **Agregar**.

11. **Ver las rutas de ataque**

Tenable Identity Exposure ofrece varias maneras de visualizar la vulnerabilidad potencial de un activo empresarial a través de representaciones gráficas.

Para obtener información completa, consulte [Ruta de ataque](#).

Acceder a la característica Ruta de ataque:

1. Inicie sesión en Tenable Identity Exposure.
2. Haga clic en el ícono de menú de la parte superior izquierda para expandir la barra de navegación.
3. En la sección **Análisis de seguridad**, haga clic en **Ruta de ataque**. La funcionalidad Ruta de ataque tiene tres modos:



- Ruta de ataque
- Radio de ataque
- Exposición de los activos

Usar el modo Radio de ataque:

1. En el cuadro de búsqueda, escriba el nombre de la cuenta (por ejemplo, "Juan Pérez").
2. Seleccione la cuenta de la lista y haga clic en el ícono de la lupa.
3. Explore el radio de ataque de la cuenta en riesgo seleccionada.
4. Filtre y consulte los nodos según sea necesario.
5. Pase el cursor por los puntos de conexión para ver la ruta de ataque.
6. Alterne la opción para mostrar toda la información sobre herramientas de los nodos.
7. Use la barra de zoom para ajustar la vista.
8. Para cambiar el objeto de búsqueda, haga clic en la **X** junto al nombre de la cuenta y haga una nueva búsqueda.

Usar el modo Exposición de los activos:

1. En el cuadro de búsqueda, escriba el nombre del servidor sensible (por ejemplo, "srv-fin").
2. Seleccione el objeto de la lista y haga clic en el ícono de la lupa.
3. Explore la exposición de los activos al servidor sensible seleccionado.
4. Use opciones similares a las del modo Radio de ataque.
5. Pase el cursor por las rutas para ver los detalles.
6. Alterne la opción para mostrar toda la información sobre herramientas de los nodos.
7. Ajuste la vista con la barra inferior.

Usar el modo Ruta de ataque:



1. En el cuadro de búsqueda del punto de entrada, escriba el nombre de la cuenta en riesgo (por ejemplo, "Juan Pérez").
2. Haga clic en el nombre de la cuenta.
3. En el cuadro de búsqueda del punto de llegada, escriba el nombre del activo sensible (por ejemplo, "s or v-fin").
4. Haga clic en el nombre del activo.
5. Haga clic en el ícono de la lupa.
6. Explore las rutas de ataque disponibles entre la cuenta en riesgo y el activo sensible.
7. Use opciones similares a las de los modos Radio de ataque y Exposición de los activos.

Capacidades adicionales:

- **¿Quién tiene el control de mis activos con privilegios?:** muestra todas las cuentas de usuario y de equipo que tienen una ruta de ataque que conduce a un activo con privilegios.
- **¿Qué son mis activos con privilegios?:** enumera los activos y cuentas de nivel cero con posibles rutas de ataque que conducen a esos activos.
- Cambie entre las pestañas para ver las listas.
- Haga clic en el ícono de la lupa junto a un elemento para cambiar la vista.
- Haga clic en el ícono de flecha azul y punto para abrir la vista de exposición de los activos filtrada para mostrar solo este activo.

Interpretar los resultados:

1. Use la característica Ruta de ataque para confirmar las hipótesis y visualizar las rutas de ataque peligrosas entre las entidades.
2. Adopte medidas correctivas para cerrar las rutas de ataque detectadas.

Sugerencia: Para obtener información adicional sobre Tenable Identity Exposure, revise los siguientes materiales de capacitación para clientes:



- [Tenable Identity Exposure Self Help Guide](#)
(Guía de autoayuda de Tenable Identity Exposure)
- [Tenable Identity Exposure Introduction \(Tenable University\)](#)
(Introducción a Tenable Identity Exposure [Tenable University])



Aspectos esenciales de Tenable Identity Exposure

En esta sección se abordan las tareas diarias fundamentales que la mayoría de los usuarios tiene que conocer para comenzar a usar Tenable Identity Exposure y aprovecharlo al máximo.

Ya sea que recién conozca el producto o simplemente necesite un repaso de los conceptos básicos, aquí encontrará instrucciones detalladas de las operaciones comunes, como la autenticación, la navegación por el espacio de trabajo, la configuración de preferencias y notificaciones, el uso de tableros de control y widgets, la exploración de las identidades con el Centro de exposición, la visualización de rastros de datos con Trail Flow y la descripción general de los indicadores de exposición e indicadores de ataque.

Para encontrar información relacionada con una tarea en particular, haga clic en los temas pertinentes en el panel de menú a la izquierda de la pantalla.

Iniciar sesión en Tenable Identity Exposure

Puede acceder a la aplicación web de Tenable Identity Exposure a través de una URL de cliente.

Para iniciar sesión en Tenable Identity Exposure, seleccione una de las siguientes opciones:

- [Usar una cuenta de Tenable Identity Exposure](#)
- [Usar una cuenta de LDAP](#)
- [Usar SAML](#)

Nota: Las credenciales iniciales tienen el nombre de usuario `hello@tenable.ad` y la contraseña `Hello@tenable.ad123!`.

Usar una cuenta de Tenable Identity Exposure

Para iniciar sesión en su cuenta de Tenable Identity Exposure :

1. En cualquier navegador, escriba la dirección URL del cliente (por ejemplo: `cliente.tenable.ad`) en la barra de direcciones.

Aparece la ventana **Iniciar sesión**.



tenable
Identity Exposure

Tenable Identity Exposure LDAP SAML

Email address client@tenable.ad

Password

Log in

2. Haga clic en la pestaña **Tenable Identity Exposure**.
3. Escriba su dirección de correo electrónico.
4. Escriba la contraseña.
5. Haga clic en **Iniciar sesión**.

Se abre la página de Tenable Identity Exposure.

Usar una cuenta de LDAP

Para iniciar sesión con LDAP:

1. En cualquier navegador, escriba la dirección URL del cliente (por ejemplo: cliente.tenable.ad) en la barra de direcciones.

Aparece la ventana **Iniciar sesión**.




tenable[®] Identity Exposure

Tenable Identity Exposure


LDAP

SAML

Email address

 client@tenable.ad

Password



Log in

2. Haga clic en la pestaña **LDAP**.
3. Escriba el nombre de su cuenta de LDAP.
4. Escriba la contraseña de LDAP.
5. Haga clic en **Iniciar sesión**.

Se abre la página de Tenable Identity Exposure.

Usar SAML

Para iniciar sesión con SAML:

1. En cualquier navegador, escriba la dirección URL del cliente (por ejemplo: cliente.tenable.ad) en la barra de direcciones.

Aparece la ventana **Iniciar sesión**.



Tenable Identity Exposure LDAP **SAML**

Email address

Password

Log in

2. Haga clic en la pestaña **SAML**.

3. Haga clic en el vínculo al proveedor de identidad (IdP).

Tenable Identity Exposure lo redirecciona al servidor SAML para la autenticación.

4. Escriba las credenciales de su empresa en el IdP.

Se lo redirigirá a Tenable Identity Exposure como usuario que inició sesión.

Precaución: Si se producen varios intentos fallidos de inicio de sesión, Tenable Identity Exposure bloqueará la cuenta. Póngase en contacto con su administrador.

Para restablecer la contraseña después del primer inicio de sesión:

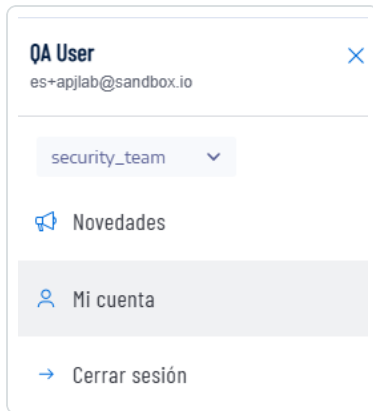
Cuando inicie sesión por primera vez con la cuenta `hello@tenable.ad`, Tenable Identity Exposure le solicitará que restablezca la contraseña predeterminada.



Nota: La información de la contraseña no está disponible si tiene una licencia de Tenable One, en cuyo caso Tenable Vulnerability Management gestiona todas las opciones de autenticación. Para obtener más información, consulte [Access Control \(Control de acceso\) en Tenable Vulnerability Management User Guide](#) (Guía del usuario de Tenable Vulnerability Management).

1. En Tenable Identity Exposure, haga clic en el ícono del perfil de usuario en la esquina superior derecha.

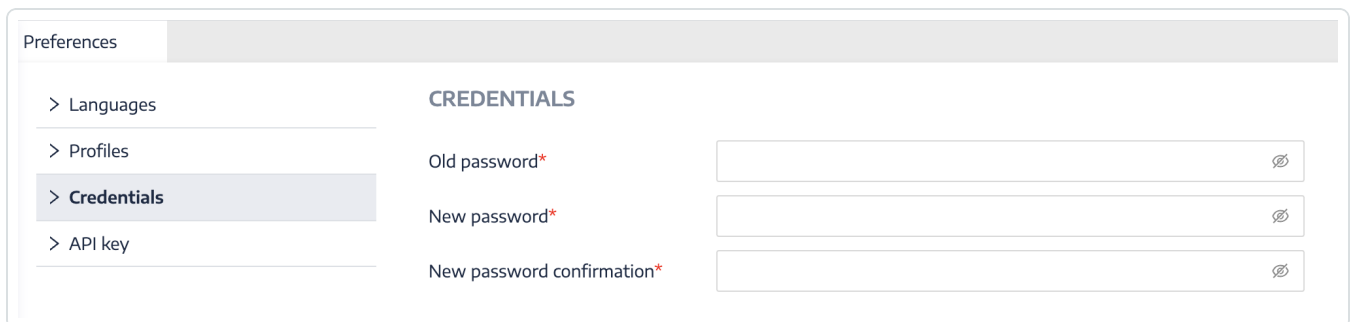
Aparece un submenú.



2. Seleccione **Mi cuenta**.

Aparece la página **Preferencias**.

3. En **Preferencias**, haga clic en **Credenciales**.



4. En **Contraseña anterior**, escriba la contraseña anterior.
5. En **Contraseña nueva**, escriba una contraseña nueva. Cumpla con las siguientes reglas de complejidad de contraseñas, que se alinean con las exigidas para las cuentas de Tenable One:



- Debe tener una longitud mínima de 12 caracteres.
- Debe contener al menos uno de cada elemento de los siguientes:
 - Letra mayúscula (A-Z)
 - Letra minúscula (a-z)
 - Número (0-9)
 - Carácter especial (por ejemplo, !, @, #, \$)
- No puede contener la cadena `verysecure` para evitar la reutilización de la contraseña predeterminada anterior (`verySecure1!`).

6. En el cuadro **Confirmación de contraseña nueva**, vuelva a escribir la nueva contraseña.

7. Haga clic en **Guardar**.

Un mensaje confirma que Tenable Identity Exposure cambió la contraseña.

Para cerrar sesión en Tenable Identity Exposure:

1. En Tenable Identity Exposure, haga clic en el ícono de usuario.

Aparece un submenú.



2. Haga clic en **Cerrar sesión**.

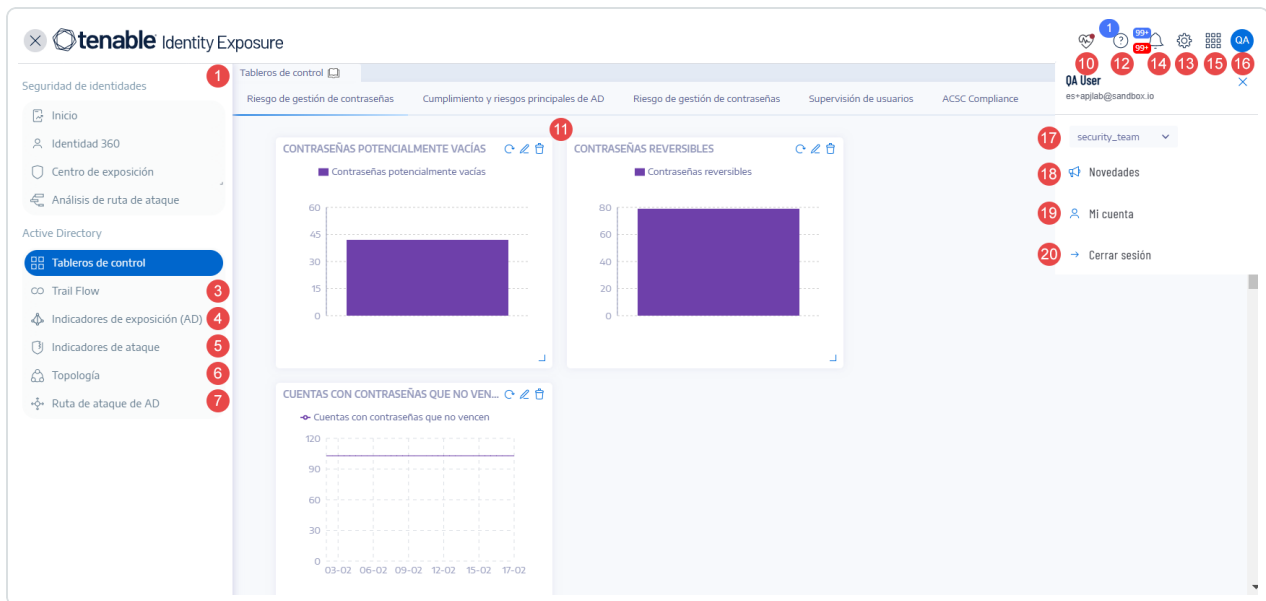
Tenable Identity Exposure vuelve a la página "Iniciar sesión".

Portal del usuario de Tenable Identity Exposure

Después de iniciar sesión en Tenable Identity Exposure, se abre la página de inicio, como se muestra en este ejemplo.

Para expandir o contraer la barra de navegación lateral:

- Para expandirla, haga clic en el menú  en la parte superior izquierda de la ventana.
- Para contraerla, haga clic en  en la parte superior izquierda de la ventana.



#	Qué es	Qué hace
1	Tableros de control	Los tableros de control le permiten administrar y supervisar de manera eficiente y visual la seguridad en una infraestructura de Active Directory.
2	-	-
3	Trail Flow	En Trail Flow se muestran la supervisión y el análisis en tiempo real de los eventos que afectan su instancia de Active Directory.
4	Indicadores de exposición	Tenable Identity Exposure usa indicadores de exposición (IoE) para medir la madurez de la seguridad de la instancia de Active Directory y para asignar niveles de gravedad (Crítico, Alto, Medio o Bajo) al flujo de eventos que se supervisan y analizan.
5	Indicadores de ataque	A través de indicadores de ataque, Tenable Identity Exposure puede



		detectar ataques en tiempo real.
6	Topología	En la página "Topología" se ofrece una visualización gráfica interactiva de su instancia de Active Directory. Se muestran los bosques, los dominios y las relaciones de confianza que existen entre ellos.
7	Ruta de ataque	En las páginas "Ruta de ataque" se ofrecen representaciones gráficas de las relaciones de Active Directory: <ul style="list-style-type: none">• Radio de ataque: evalúa los movimientos laterales en la instancia de AD desde un activo potencialmente en riesgo.• Ruta de ataque: prevé las técnicas de escalamiento de privilegios para alcanzar un activo desde un punto de entrada específico.• Exposición de los activos: mide la vulnerabilidad de un activo mediante la visualización de la exposición del activo y aborda todas las rutas de escalamiento.
8, 9	Gestión <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;">Rol de usuario obligatorio: usuario de la organización con permisos apropiados.</div>	Esta sección le permite configurar lo siguiente: <ul style="list-style-type: none">• Cuentas: cuentas de usuario, roles y perfiles de seguridad.• Sistema: bosques y dominios,



		<p>servicios de aplicaciones, alertas y autenticación.</p> <p>Para obtener más información, consulte Configuración y administración de Tenable Identity Exposure.</p>
10	Verificaciones de estado	Las verificaciones de estado le brindan visibilidad en tiempo real de la configuración de los dominios y las cuentas de servicio en una vista consolidada desde la que puede profundizar para obtener información más detallada.
11	Widgets	Los widgets son conjuntos de datos personalizables en un tablero de control. Pueden contener gráficos de barras, gráficos de líneas y contadores.
12	Actualizaciones del producto	Información sobre las características más recientes del producto.
13	Configuración	Acceso a la configuración del sistema; la gestión de bosques y dominios; la gestión de licencias, usuarios y roles; perfiles y registros de actividad.
14	Notificaciones (campana)	Un ícono de campana y los conteos de insignias le notifican sobre alertas de ataque o alertas de exposición que están a la espera de que les preste atención.
15	Acceder a "Espacio de trabajo"	Haga clic en este ícono para alternar



		entre las aplicaciones desde el espacio de trabajo de Tenable.
16, 19	Ícono de perfil de usuario (Preferencias del usuario)	Haga clic en este ícono para acceder a un submenú de perfiles de seguridad, notas de la versión, registros de actividad, preferencias o cerrar sesión.
17	Perfiles de seguridad	Los perfiles de seguridad permiten que distintos tipos de usuarios revisen el análisis de seguridad desde diferentes ángulos de informes.
18	Novedades	Haga clic para abrir las notas de la versión más reciente de Tenable Identity Exposure.
20	Cerrar sesión	Haga clic para cerrar la sesión de Tenable Identity Exposure.

Acceder a “Espacio de trabajo”


Cuando inicia sesión en Tenable, la página **Espacio de trabajo** aparece de manera predeterminada. En la página **Espacio de trabajo**, puede cambiar entre sus aplicaciones de Tenable o configurar una aplicación predeterminada para omitir la página **Espacio de trabajo** en el futuro. También puede cambiar entre las aplicaciones desde el menú **Espacio de trabajo**, que aparece en la barra de navegación superior.

Importante: Tenable deshabilita los mosaicos de las aplicaciones vencidas. Tenable quita los mosaicos de las aplicaciones vencidas de la página **Espacio de trabajo** y del menú 30 días después del vencimiento.

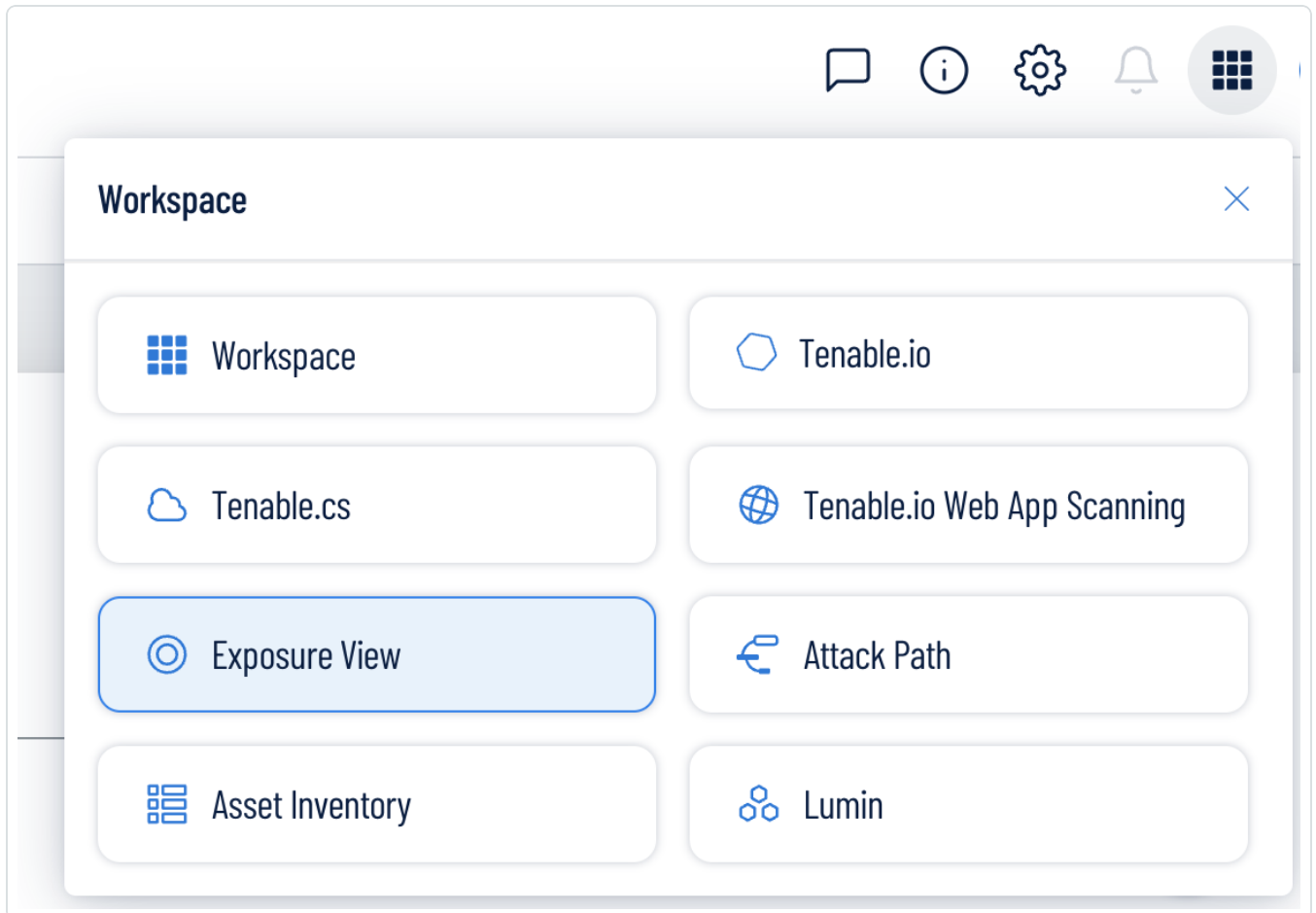
Abrir el menú “Espacio de trabajo”

Para abrir el menú **Espacio de trabajo**:



1. Desde cualquier aplicación de Tenable, en la esquina superior derecha, haga clic en el botón .

Aparece el menú **Espacio de trabajo**.



2. Haga clic en el mosaico de una aplicación para abrirla.

Ver la página “Espacio de trabajo”

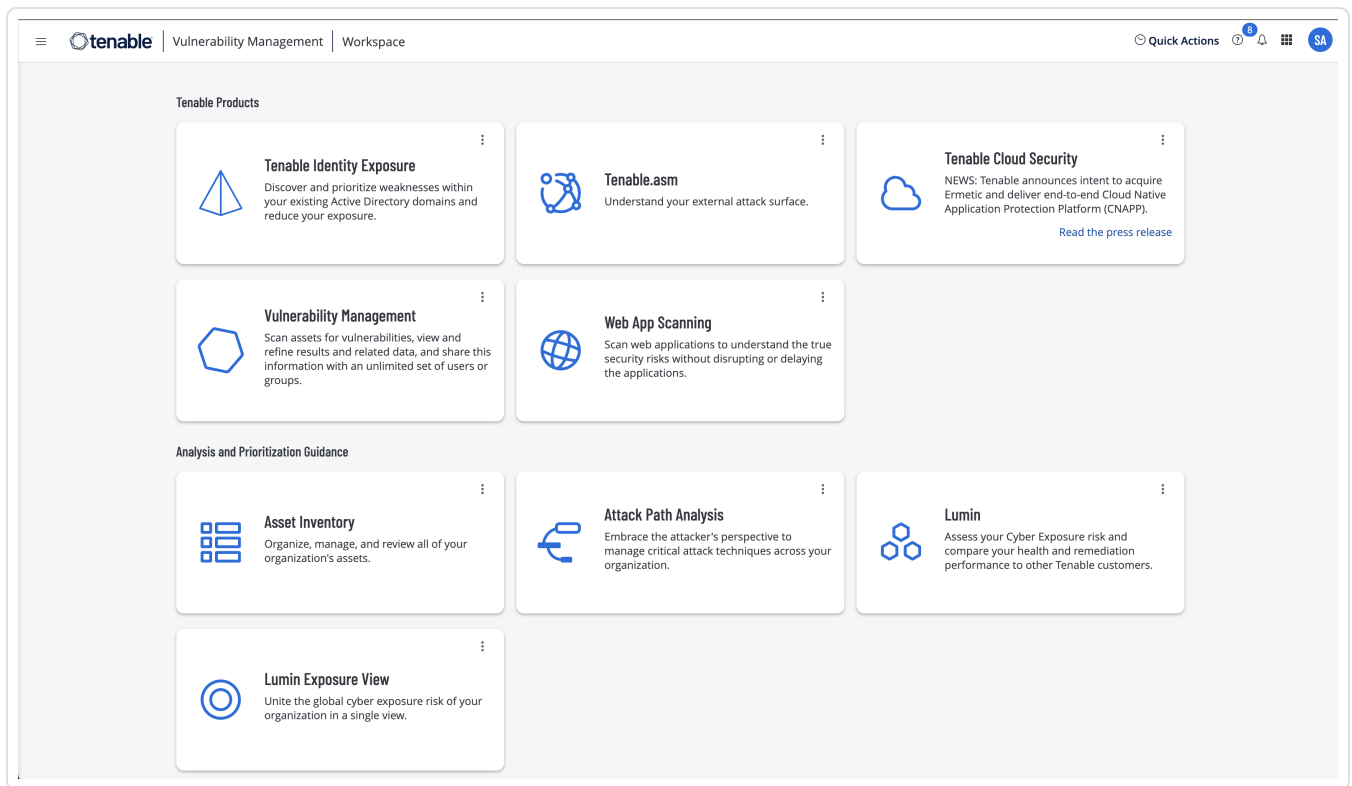
Para ver la página “Espacio de trabajo”:

1. Desde cualquier aplicación de Tenable, en la esquina superior derecha, haga clic en el botón .

Aparece el menú **Espacio de trabajo**.

2. En el menú **Espacio de trabajo**, haga clic en **Espacio de trabajo**.

Aparece la página **Espacio de trabajo**.



Establecer una aplicación predeterminada

Cuando inicia sesión en Tenable, la página **Espacio de trabajo** aparece de manera predeterminada. Sin embargo, puede definir una aplicación predeterminada para omitir la página **Espacio de trabajo** en el futuro.

De manera predeterminada, los usuarios con los roles **Administrador**, **Administrador de escaneo**, **Operador de escaneo**, **Estándar** y **Básico** pueden definir una aplicación predeterminada. Si tiene otro rol, comuníquese con su administrador y solicite el permiso **Gestionar** en **Mi cuenta**. Para obtener más información, consulte [Custom Roles](#) (Roles personalizados).

Para establecer una aplicación de inicio de sesión predeterminada:

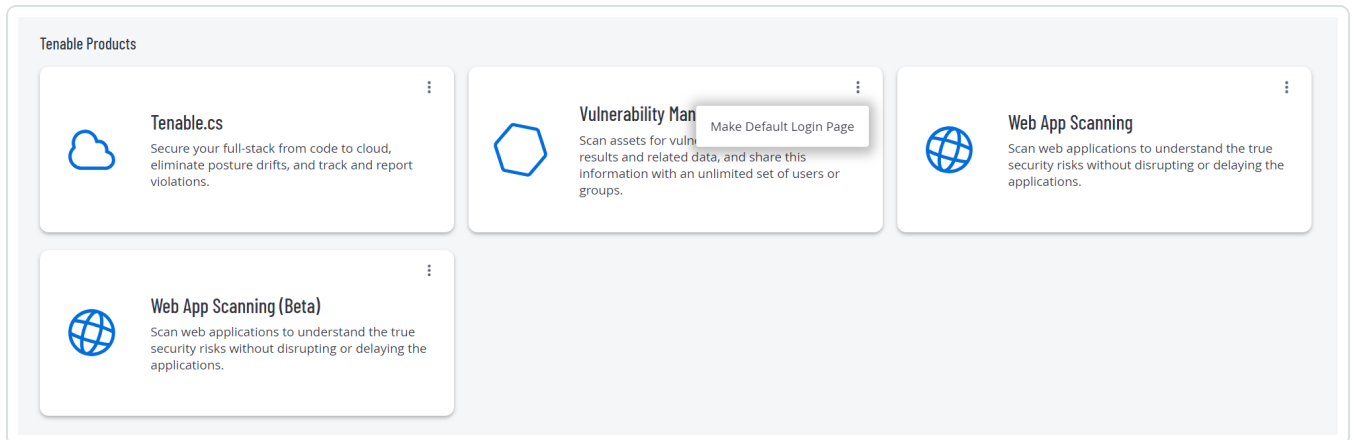
1. Inicie sesión en Tenable.

Aparece la página **Espacio de trabajo**.

2. En la esquina superior derecha de la aplicación que quiere elegir, haga clic en el botón **⋮**.



Aparece un menú.



3. En el menú, haga clic en **Convertir en página de inicio de sesión predeterminada**.

Cuando inicia sesión, ahora aparece esta aplicación.

Quitar una aplicación predeterminada

Para quitar una aplicación de inicio de sesión predeterminada:

1. Inicie sesión en Tenable.

Aparece la página **Espacio de trabajo**.

2. En la esquina superior derecha de la aplicación que quiere quitar, haga clic en el botón **⋮**.

Aparece un menú.

3. Haga clic en **Quitar página de inicio de sesión predeterminada**.

Cuando inicia sesión, ahora aparece la página **Espacio de trabajo**.

Preferencias del usuario

En Tenable Identity Exposure, puede establecer sus preferencias de usuario.

- [Para seleccionar el idioma:](#)
- [Para seleccionar su perfil:](#)

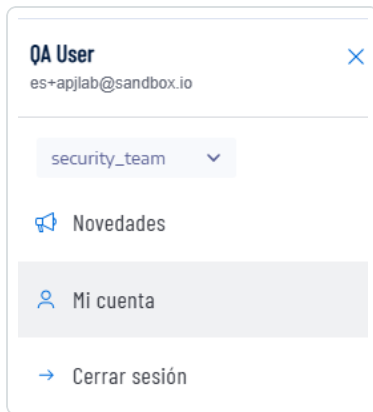


- [Para cambiar la contraseña:](#)
- [Para seleccionar su perfil:](#)

Para establecer sus preferencias:

1. En Tenable Identity Exposure, haga clic en el ícono del perfil de usuario en la esquina superior derecha.

Aparece un submenú.



2. Seleccione **Mi cuenta**.

Aparece la página **Preferencias**.

Para seleccionar el idioma:

- a. En **Idiomas**, haga clic en la flecha de la lista desplegable para seleccionar el idioma preferido.
- b. Haga clic en **Guardar**.

Un mensaje confirma que Tenable Identity Exposure actualizó las preferencias. La interfaz de usuario aparece en el idioma que seleccionó.

Para seleccionar su perfil:

Al cambiar de un perfil de seguridad a otro, se modifica la forma en que Tenable Identity Exposure muestra la configuración de los indicadores y la representación de los datos en los tableros de control, los widgets y Trail Flow.



- a. En **Preferencias**, haga clic en **Perfiles**.
- b. En **Perfil de preferencia**, haga clic en la flecha desplegable para seleccionar su perfil predeterminado después de conectarse a Tenable Identity Exposure.
- c. Haga clic en **Guardar**.

Un mensaje confirma que Tenable Identity Exposure actualizó las preferencias.

Para obtener más información, consulte [Perfiles de seguridad](#).

Para cambiar la contraseña:

Nota: La información de la contraseña no está disponible si tiene una licencia de Tenable One, en cuyo caso Tenable Vulnerability Management gestiona todas las opciones de autenticación. Para obtener más información, consulte [Access Control \(Control de acceso\) en Tenable Vulnerability Management User Guide](#) (Guía del usuario de Tenable Vulnerability Management).

- a. En **Preferencias**, haga clic en **Credenciales**.
- b. En **Contraseña anterior**, escriba la contraseña anterior.
- c. En **Contraseña nueva**, escriba una contraseña nueva. Cumpla con las siguientes reglas de complejidad de contraseñas, que se alinean con las exigidas para las cuentas de Tenable One:
 - Debe tener una longitud mínima de 12 caracteres.
 - Debe contener al menos uno de cada elemento de los siguientes:
 - Letra mayúscula (A-Z)
 - Letra minúscula (a-z)
 - Número (0-9)
 - Carácter especial (por ejemplo, !, @, #, \$)
 - No puede contener la cadena `verysecure` para evitar la reutilización de la contraseña predeterminada anterior (`verySecure1!`).
- d. En el cuadro **Confirmación de contraseña nueva**, vuelva a escribir la nueva contraseña.
- e. Haga clic en **Guardar**.

Un mensaje confirma que Tenable Identity Exposure cambió la contraseña.




Nota: No puede cambiar una contraseña de cuentas conectadas a través de proveedores externos, como LDAP o SAML, en Tenable Identity Exposure.

Para administrar la clave de API:

- a. En **Preferencias**, haga clic en **Clave de API**.

El token de acceso aparece en el cuadro **Clave de API actual**.

- b. Puede hacer lo siguiente:

- c. Haga clic en el ícono  para copiar la clave de API en el portapapeles para usarla cuando sea necesario.

- d. Haga clic en **Actualizar clave de API** para generar un nuevo token de acceso.


Aparece un mensaje para pedirle la confirmación.

Nota: Al actualizar la clave de API, Tenable Identity Exposure desactivará el token actual.

Para obtener más detalles, consulte [Usar API pública](#).

Notificaciones

En la esquina superior derecha de la página de inicio de Tenable Identity Exposure, un ícono de campana y los conteos de insignias le notifican sobre alertas de ataque o alertas de exposición que están a la espera de que les preste atención. Cuando recibe nuevas alertas, Tenable Identity Exposure aumenta los conteos de insignias de notificación.

	Azul	Alertas de exposición
	Rojo	Alertas de ataque

Para mostrar las alertas:

1. En Tenable Identity Exposure, haga clic en el ícono de la campana.

Se abre el panel **Alertas**.

2. Siga uno de los procedimientos a continuación:



- Haga clic en la pestaña **Alertas de exposición** para mostrar las alertas de exposición.
 - Haga clic en la pestaña **Alertas de ataque** para mostrar las alertas de ataque.
- Aparece una lista de alertas asociadas.

Para ver el evento asociado a la alerta:

1. Seleccione una alerta de la lista y haga clic en **Acciones > Ver la anomalía**.

El panel “Detalles del evento” se abre con la siguiente información:

- Origen (recopilador de eventos)
- Tipo de objeto
- Archivo
- Ruta
- Dominios afectados
- Fecha
- Una lista de atributos con valores en el momento del evento y el valor actual

2. Haga clic en la pestaña **Anomalías**.

Se abre el panel **Anomalías**, donde se muestra una lista de anomalías asociadas al evento.

The screenshot displays the Tenable Identity Exposure web interface. The main content area is titled "Detalles del evento" and shows a table with columns: ORIGEN (SYSVOL), TIPO (New object), ARCHIVO (Carpeta), RUTA GLOBAL, DOMINIOS AFECTADOS (ALSID.CORP Forest (prod), Japan Domain @ Alsid.corp), and FECHA DEL EVENTO (06:47:28, 2022-09-07). Below the table, the "Anomalías" section is active, showing a warning icon and the text "Permisos inseguros definidos en el objeto o archivo de GPO". The description states: "El GPO Default: Domain Controllers Policy está vinculado a los contenedores de este GPO tiene entradas peligrosas en el descriptor de seguridad de del GPO. Las ACE peligrosas son las siguientes: (alsid.corp)Ben Angel". A list of permissions is shown: File write, Delete subfolders and files, Create folders, and Create files. At the bottom, a red box highlights "Controladores de dominio administrados por usuarios legítimos". On the right side, there are two green circles: one around "1/1 indicador >" and another around "1/1 motivo >".

3. Haga clic en **n/n indicadores** para mostrar el panel del indicador de exposición que desencadenó la alerta.



4. Haga clic en **n/n motivos** para mostrar los motivos de la alerta.
5. Haga clic en la flecha para expandir o contraer la información de la alerta.
6. Haga clic en el nombre del indicador para mostrar la página “Detalles del indicador”.

Para archivar la alerta:

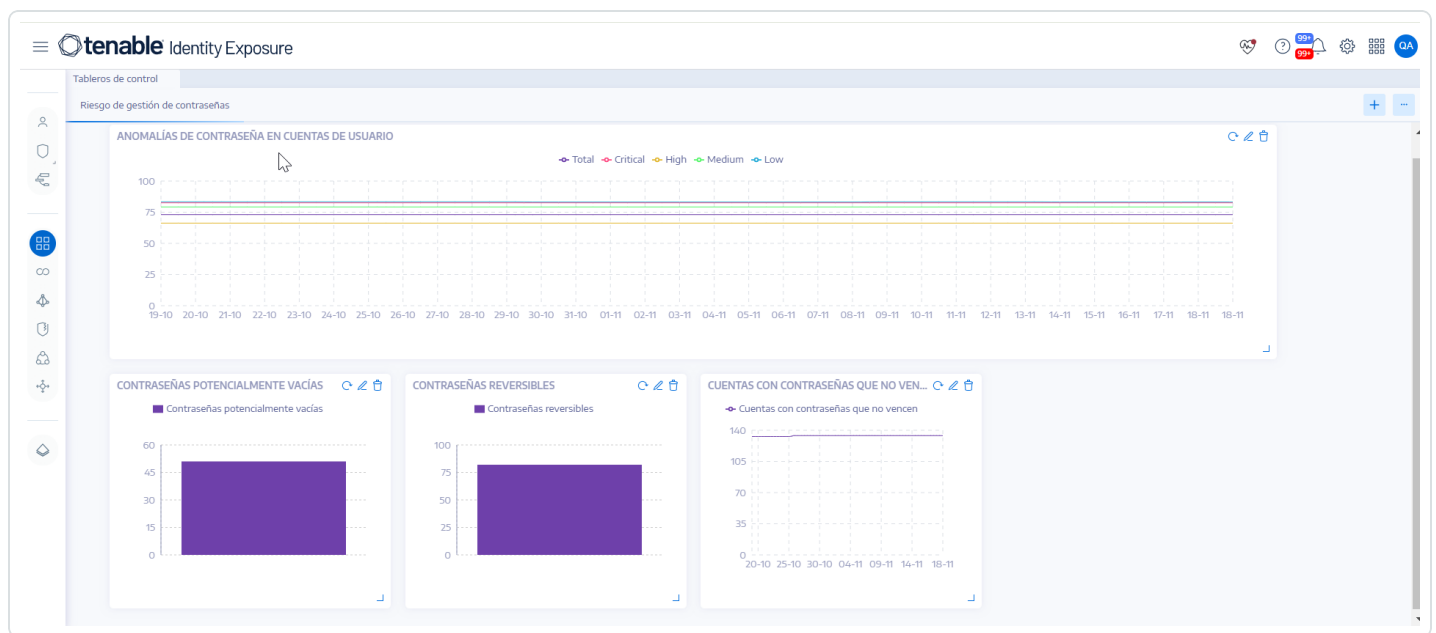
Después de ver la alerta, puede archivarla.

1. En la lista de alertas del panel **Alertas**, seleccione la casilla de la alerta que quiere archivar.
 - De manera opcional, puede hacer clic en la casilla **n/n objetos seleccionados** al final del panel para seleccionar todas las alertas de forma masiva.
2. Al final del panel, haga clic en **Seleccionar una acción > Archivar**.
3. Haga clic en **Aceptar**.

Tableros de control

Los tableros de control le permiten visualizar datos y tendencias que afectan la seguridad de su instancia de Active Directory. Puede personalizarlos con widgets para mostrar gráficos y contadores según sus requisitos.

El tablero de control de Tenable Identity Exposure sirve como centro de comando en tiempo real para la seguridad de Active Directory (AD) de su organización. Ofrece una descripción general completa (por ejemplo, una vista centralizada en tiempo real) de su panorama de identidades, donde se destacan vulnerabilidades críticas, se detectan posibles vectores de ataque y se permite la mitigación proactiva de riesgos.



Funcionalidades clave de los tableros de control

- **Generalidades de un vistazo:** conozca rápidamente su estado de seguridad con métricas clave que se muestran de manera destacada, como la puntuación de cumplimiento, los principales riesgos y las tendencias de actividad de los usuarios.
- **Análisis de los detalles:** profundice en áreas específicas con widgets interactivos que desglosan los factores de riesgo por gravedad, categoría de usuario y otros criterios pertinentes.
- **Enfoque personalizable:** cree tableros de control personalizados adaptados a sus prioridades; para ello, puede usar plantillas prediseñadas o crear sus propios diseños. Por ejemplo, para crear un tablero de control de los errores de configuración más comunes frente a los loE recurrentes más comunes:
 - Asegurar la coherencia de SDProp.
 - Controladores de dominio administrados por usuarios ilegítimos.
 - Delegación peligrosa de Kerberos.
- **Supervisión en tiempo real:** manténgase al tanto de las amenazas emergentes y la actividad sospechosa por medio de actualizaciones y alertas continuas.



- **Información accionable:** obtenga recomendaciones prácticas para la corrección, priorizadas según la gravedad y el posible impacto.

Plantillas de tableros de control

Tenable Identity Exposure proporciona plantillas de tableros de control que se pueden usar para centrarse en cuestiones prioritarias que afectan a la organización, incluidas las siguientes plantillas:


- **Cumplimiento y riesgos principales de AD:** puntuación de cumplimiento, evolución y criticidad del riesgo.
- **Riesgo de AD 360:** evolución de las anomalías y los problemas según el nivel de gravedad del indicador de exposición.
- **Riesgo de gestión de contraseñas:** problemas relacionados con las contraseñas.
- **Supervisión de usuarios:** evolución de los usuarios de AD, conteo de categorías de usuarios.
- **Supervisión nativa de administradores:** métricas de cuentas administrativas.

Para crear un nuevo tablero de control con una plantilla:

1. En Tenable Identity Exposure, haga clic en  o en **Tableros de control**. (Esta página también se abre de manera predeterminada en Tenable Identity Exposure).
2. Puede seguir cualquiera de los siguientes procedimientos:
 - Si el panel está vacío, haga clic en **Agregar tableros de control**.
 - Si el panel ya contiene al menos un tablero de control, haga clic en  > **Agregar nuevo tablero de control** en la esquina superior derecha.
Se abre el panel **Configurar plantillas de tableros de control**.
3. Seleccione los tableros de control que quiere agregar.
4. Haga clic en **Agregar tableros de control**.
5. Un mensaje confirma que Tenable Identity Exposure creó el tablero de control y los widgets. Los nuevos tableros de control aparecen en una pestaña en el panel **Tableros de control**.



Para agregar un tablero de control personalizado:

1. En Tenable Identity Exposure, haga clic en  o en **Tableros de control**. (Esta página también se abre de manera predeterminada en Tenable Identity Exposure).

2. Haga clic en  > **Agregar nuevo tablero de control** en la esquina superior derecha.

Se abre el panel **Configurar plantillas de tableros de control**.

3. Seleccione la plantilla **Tablero de control personalizado** al final.

4. Escriba un nombre para el tablero de control.

5. Haga clic en **Agregar tableros de control**.

Un mensaje confirma que Tenable Identity Exposure creó el tablero de control. Los nuevos tableros de control aparecen en una pestaña en el panel **Tableros de control**.

6. Consulte [Widgets](#) para obtener información sobre cómo agregar widgets a un tablero de control.

Para cambiar el nombre de un tablero de control:

1. En el panel **Tableros de control**, seleccione la pestaña del tablero de control cuyo nombre quiere cambiar.

2. Haga clic en  > **Editar nombre** en la esquina superior derecha.

Se abre el panel **Configurar el tablero de control**.

3. En el cuadro **Nombre**, escriba otro nombre para el tablero de control.

4. Haga clic en **Editar**.

Un mensaje confirma que Tenable Identity Exposure actualizó el tablero de control.

Para eliminar un tablero de control:

1. En el panel **Tableros de control**, seleccione la pestaña del tablero de control que quiere eliminar.



- Haga clic en  > **Eliminar tablero de control** en la esquina superior derecha.

Se abre el panel **Eliminar el tablero de control** para pedirle que confirme la eliminación.

- Haga clic en **Eliminar**.



Un mensaje confirma que Tenable Identity Exposure eliminó el tablero de control.

Widgets

Los widgets en los tableros de control le permiten visualizar los datos de Active Directory en forma de gráficos de barras, gráficos de líneas y contadores. Puede personalizar los widgets para mostrar información específica y arrastrarlos para reubicarlos en el tablero.

Puede agregar widgets a un tablero recién creado o a uno existente.

Para agregar un widget a un tablero de control:

- En Tenable Identity Exposure, haga clic en  o en **Tableros de control**. (Esta página también se abre de manera predeterminada en Tenable Identity Exposure).
- En el panel "Tableros de control", seleccione la pestaña del tablero de control.
- Puede seguir uno de los procedimientos a continuación:
 - Si el tablero de control está vacío, haga clic en **Agregar widgets**.
 - Si el tablero de control ya contiene widgets, haga clic en  > **Agregar widget al tablero de control actual** en la esquina superior derecha.

Se abre el panel **Agregar un widget**.
- Haga clic en un mosaico para seleccionar una de las siguientes opciones:
 - Gráfico de barras
 - Gráfico de líneas
 - Contador



5. En el cuadro **Nombre del widget**, escriba un nombre para el widget.
6. En **Configuración del widget**, en el cuadro **Tipo de datos**, haga clic en la flecha de la lista desplegable para seleccionar una de las siguientes opciones:
 - Conteo de usuarios: cantidad de usuarios activos del dominio.
 - Conteo de anomalías: cantidad de anomalías o vulneraciones de seguridad detectadas.
 - Puntuación de cumplimiento: puntuación del 0 al 100 que Tenable Identity Exposure calcula en función del número de anomalías detectadas y sus niveles de gravedad.
 - Duración (para un gráfico de líneas): haga clic en la flecha de la lista desplegable para seleccionar la duración que quiere mostrar.



7. En **Configuración de conjuntos de datos**:

Configuración de conjuntos de datos	
Estado (Conteo de usuarios)	Seleccione Activo, Inactivo o Todos.
Indicadores	<p>a. Haga clic en Indicadores para seleccionar uno o más indicadores.</p> <p>Se abre el panel Indicadores de exposición.</p> <p>b. Seleccione de la lista uno o varios indicadores. De manera opcional, también puede:</p> <ul style="list-style-type: none">■ Escribir el nombre de un indicador en el cuadro de búsqueda.■ Seleccione todos los indicadores.■ Seleccionar todos los indicadores de un nivel de gravedad específico (Crítico, Alto, Medio o Bajo). <p>c. Haga clic en Filtrar selección.</p>
Dominios	<p>a. Haga clic en Dominios para seleccionar uno o más dominios.</p> <p>Se abre el panel Bosques y dominios.</p> <p>b. Seleccione un dominio de la lista. De manera opcional, también puede:</p> <ul style="list-style-type: none">■ Escribir el nombre de un dominio en el cuadro de búsqueda.■ Seleccionar todos los dominios. <p>c. Haga clic en Filtrar selección.</p>

8. En **Nombre del conjunto de datos**, escriba un nombre para el conjunto de datos.

9. Seleccione el dominio para el widget.




De manera opcional, escriba el nombre de un dominio en el cuadro de búsqueda.

10. Haga clic en **Filtrar selección**.
11. De manera opcional, puede hacer clic en **Agregar un nuevo conjunto de datos** para agregar otro conjunto de datos con opciones diferentes para el widget.
12. Haga clic en **Agregar**.

Un mensaje confirma que Tenable Identity Exposure agregó el widget.

Para modificar un widget:


1. En Tenable Identity Exposure, haga clic en **Tableros de control**.
2. Seleccione el tablero de control que contiene el widget que quiere modificar.
3. Seleccione el widget.
4. Haga clic en el ícono  en la esquina superior derecha del widget.

Se abre el panel **Modificar un widget**.

5. Haga las modificaciones que considere necesarias.
6. Haga clic en **Editar**.

Un mensaje confirma que Tenable Identity Exposure actualizó el widget.

Para actualizar un widget:

1. Seleccione el widget.
2. Haga clic en el ícono  en la esquina superior derecha del widget.

El widget se actualiza.

Para eliminar un widget:

1. En Tenable Identity Exposure, haga clic en **Tableros de control**.
2. Seleccione el tablero de control que contiene el widget que quiere eliminar.
3. Seleccione el widget.



4. Haga clic en el ícono .

Se abre el panel “Quitar un widget”. Aparece un mensaje para pedirle que confirme la eliminación.

5. Haga clic en **Aceptar**.

Un mensaje confirma que Tenable Identity Exposure eliminó el widget del tablero de control.

Consulte también

- [Tableros de control](#)

Centro de exposición

El **Centro de exposición** es una funcionalidad de Tenable Identity Exposure que mejora la posición de seguridad de identidades de su organización. Identifica debilidades y errores de configuración en toda la superficie de riesgo de identidades y cubre los sistemas de identidades subyacentes, como Entra ID, y las identidades de esos sistemas.

La experiencia del usuario de esta funcionalidad gira en torno a tres conceptos interconectados: **Información general sobre la exposición, Instancias de exposición y Hallazgos**. Tenable Research respalda estos conceptos con **un nuevo motor de seguridad** e indicadores de exposición (IoE) desarrollados de forma específica para impulsar su funcionalidad.

- **Información general sobre la exposición**, al igual que la vista de indicadores de exposición (IoE) en Tenable Identity Exposure, representa posibles debilidades o errores de configuración que los atacantes podrían explotar. Se trata de descripciones generales de riesgos de seguridad, como “cuentas de usuario inactivas” o “permisos de acceso mal configurados”. Los IoE resaltan las áreas de exposición de forma proactiva, lo que ofrece a las organizaciones una visión integral de su posición de seguridad.
- Las **instancias de exposición** son casos específicos de estas debilidades generales. Por ejemplo, la debilidad general de “cuentas de usuario inactivas” puede tener un escenario específico, como “cuentas de usuario inactivas durante más de 30 días en el departamento de Marketing”.
- Los **hallazgos** son los resultados del análisis de las instancias de exposición frente a datos reales en diversos orígenes de datos de identidades. Un hallazgo representa un problema de



seguridad en un activo afectado, identificado de forma única por atributos como el usuario, el grupo y el rol. Por ejemplo, si una cuenta de usuario está inactiva durante un tiempo mayor al umbral especificado en la instancia de exposición, se marcará como un hallazgo.

El proceso comienza con una biblioteca de debilidades que se aplica continuamente a sus proveedores de identidad a través de escaneos.

Tenable Research proporciona debilidades predeterminadas y las actualiza de forma continua para hacer un seguimiento del escenario de las amenazas. Estas debilidades, adaptadas a sus necesidades específicas en instancias de exposición, generan hallazgos que luego se presentan junto con puntuaciones de gravedad y pautas de corrección. Al aprovechar esta funcionalidad, Tenable Identity Exposure ayuda a las organizaciones a mitigar de forma proactiva los riesgos de seguridad.

Nota: El Centro de exposición solo presenta las debilidades que el nuevo motor de seguridad admite. Los indicadores de exposición (IoE) generados por el motor de seguridad más antiguo no aparecen aquí. Sin embargo, los IoE de Active Directory (AD) actuales siguen estando visibles en la página de indicadores de exposición de Tenable Identity Exposure.

Requisitos previos

- Para usar el **Centro de exposición** en Tenable Identity Exposure, habilite la opción **Activar compatibilidad de Identidad 360 con el Centro de exposición y Microsoft Entra ID** en “Configuración del sistema”.
- **(Opcional)** Para aprovechar las debilidades de Active Directory, habilite la recopilación de datos en Tenable Cloud.



Precaución: Para utilizar esta funcionalidad, **no debe** aplicar el filtrado de direcciones IP en Tenable Vulnerability Management para permitir el acceso de la API a Tenable Identity Exposure. Consulte [API Access Security](#) (Seguridad de acceso a la API) para obtener más información.

Consulte también

- [Información general sobre la exposición](#)
- [Instancias de exposición](#)

Información general sobre la exposición


Tenable Identity Exposure proporciona visibilidad integral de las debilidades y los errores de configuración en varios proveedores de identidad, incluidos Active Directory (AD) y Entra ID.

Al analizar de forma continua las cuentas privilegiadas, las políticas de contraseñas o las configuraciones de delegación, entre otros recursos, e identificar debilidades críticas, Tenable Identity Exposure permite a las organizaciones corregir las brechas de seguridad de manera proactiva.

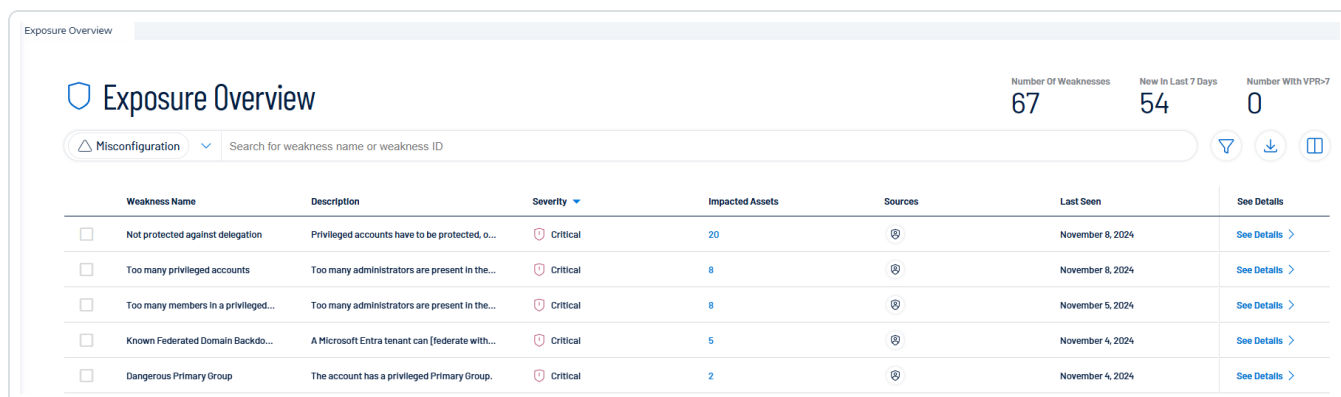
Esta información general le permite priorizar los problemas según la gravedad, los activos afectados y la detección reciente, lo que garantiza un enfoque específico y eficiente para la gestión de la seguridad de identidades.



Para acceder a la página **Información general sobre la exposición**:

1. En el panel de navegación izquierdo de Tenable Identity Exposure, haga clic en el ícono del Centro de exposición .
2. En el submenú, haga clic en **Información general sobre la exposición**.

Aparece la página **Información general sobre la exposición**.



Exposure Overview							Number Of Weaknesses	New In Last 7 Days	Number With VPR-7
Misconfiguration							67	54	0
Weakness Name	Description	Severity	Impacted Assets	Sources	Last Seen	See Details			
<input type="checkbox"/> Not protected against delegation	Privileged accounts have to be protected, o...	Critical	20		November 8, 2024	See Details >			
<input type="checkbox"/> Too many privileged accounts	Too many administrators are present in the...	Critical	8		November 8, 2024	See Details >			
<input type="checkbox"/> Too many members in a privileged...	Too many administrators are present in the...	Critical	8		November 5, 2024	See Details >			
<input type="checkbox"/> Known Federated Domain Backdo...	A Microsoft Entra tenant can federate with...	Critical	5		November 4, 2024	See Details >			
<input type="checkbox"/> Dangerous Primary Group	The account has a privileged Primary Group.	Critical	2		November 4, 2024	See Details >			

Información del encabezado

- **Cantidad de debilidades**: muestra el total de debilidades detectadas.
- **Nuevas en los últimos 7 días**: destaca las nuevas debilidades detectadas en la última semana.

Lista de debilidades

En la lista de debilidades aparecen las siguientes columnas:

- **Nombre de la debilidad**: indica debilidades o errores de configuración específicos que se detectaron. Ejemplo: "Sin protección frente a la delegación", "Demasiadas cuentas privilegiadas", etc.
- **Descripción**: proporciona una breve explicación del problema. Ejemplo: "Las cuentas privilegiadas deben protegerse...", "Hay demasiados administradores presentes..."
- **Gravedad**: muestra la criticidad de cada debilidad (crítica, alta, media, baja).
- **Activos afectados**: muestra la cantidad de activos afectados por cada debilidad.



- **Orígenes:** muestra los sistemas o las plataformas que detectaron los datos. Estos datos pueden provenir de varios productos.
- **Última visualización:** muestra la última vez que se detectó o informó cada debilidad. Ejemplo: "10 de septiembre de 2024", "29 de septiembre de 2024".
- **Ver los detalles:** le permite ver más información sobre cada debilidad.

Sugerencia: La flecha de "Ver los detalles" le lleva a Tenable Inventory. Para obtener información más detallada sobre la debilidad específica, consulte [Weaknesses in Tenable Inventory](#) (Debilidades en Tenable Inventory).

Nota: La funcionalidad Información general sobre la exposición actualmente muestra datos relacionados con debilidades según el **perfil predeterminado de Tenable** y no refleja automáticamente el **estado de las anomalías en los objetos de AD que se permitieron en otros perfiles**.

Por lo tanto:

- Si **permitió un objeto de AD** para un indicador de exposición en particular (por ejemplo, "Miembro de grupos administrativos nativos"), **Información general sobre la exposición aún lo marcará como una debilidad de seguridad si el perfil predeterminado lo identificó como anómalo**.
- Esto puede generar la impresión de que el problema no se ha abordado, aunque el objeto ya se haya permitido con otro perfil.
- Si se adopta una medida correctiva (como eliminar la membresía al grupo) según lo que se ve en Información general sobre la exposición, el objeto desaparecerá de la vista, pero esto podría no haber sido necesario si el objeto ya se hubiera permitido en otro lugar.

Opciones de búsqueda, filtrado, exportación y visualización de columnas

Filtrar

Una función de filtro en **Información general sobre la exposición** le permite aplicar criterios específicos para acotar o ajustar los datos que aparecen.

Para aplicar un filtro en la lista de debilidades:

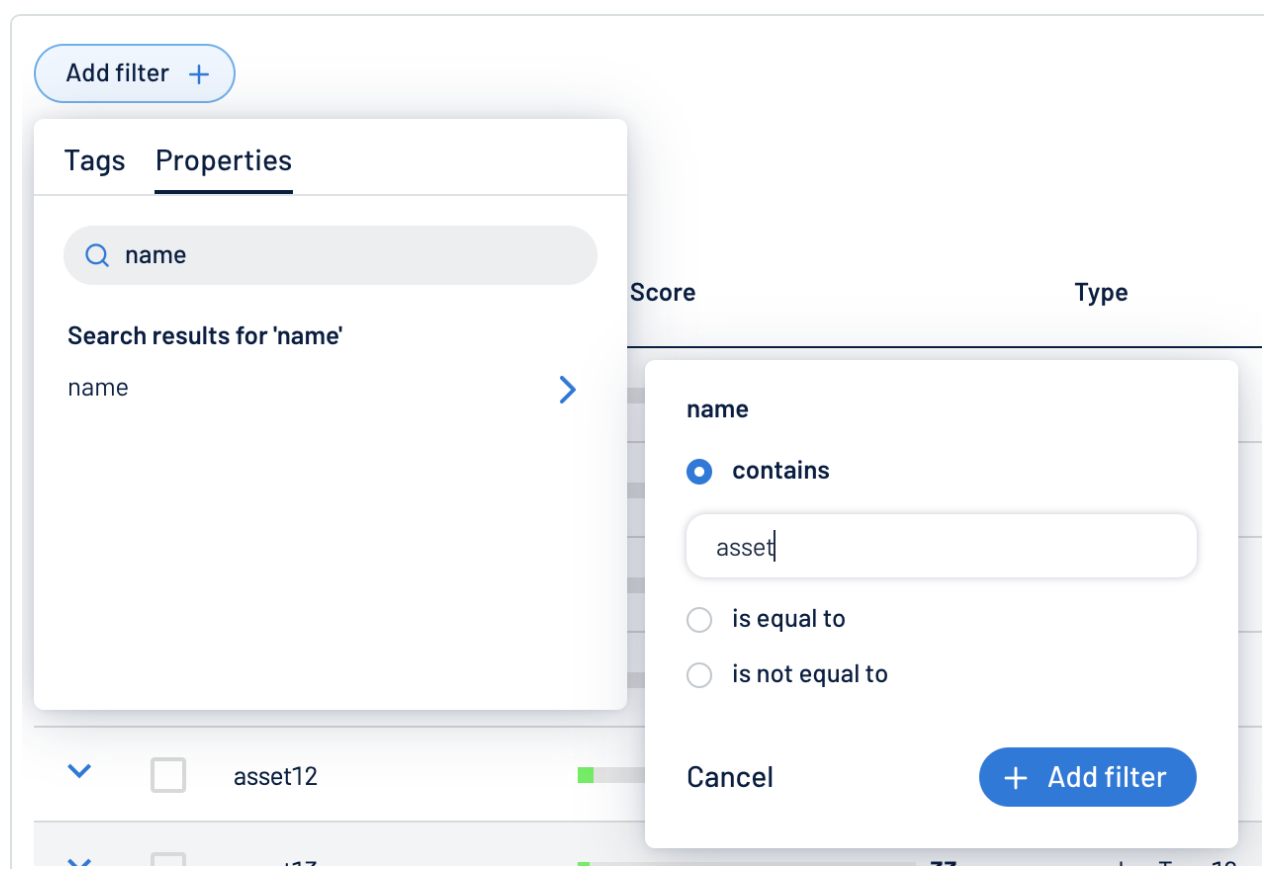


1. En el encabezado de la página **Información general sobre la exposición**, haga clic en el ícono .

Aparece el botón “Agregar filtro”.

2. Haga clic en **Agregar filtro +**.

Aparece un menú.



3. Siga uno de los procedimientos a continuación:
 - Para buscar en la lista de debilidades por etiqueta, haga clic en **Etiquetas** (solo rige con la licencia de Tenable One y se gestiona en Tenable Inventory).
 - Para buscar en la lista de debilidades por propiedad, haga clic en **Propiedades**.
4. En el cuadro de búsqueda, escriba los criterios por los cuales quiere buscar.

Tenable Inventory rellena una lista de opciones según los criterios.
5. Haga clic en la etiqueta o propiedad por la que quiere filtrar la lista de debilidades.



Aparece un menú.

6. Seleccione cómo aplicar el filtro. Por ejemplo, si quiere buscar una debilidad cuyo nombre es "Weakness14", seleccione el botón de selección "contiene" y, en el cuadro de texto, escriba "Weakness14".

7. Haga clic en **Agregar filtro**.

El filtro aparece encima de la lista de debilidades.

8. Repita estos pasos para cada filtro adicional que quiera aplicar.


9. Haga clic en **Aplicar filtros**.

La página filtra la lista de identidades según los criterios designados.

Exportar

Puede exportar los datos que aparecen en la tabla a un archivo de Excel.

Para exportar datos:

1. En el encabezado de la página **Información general sobre la exposición**, haga clic en el ícono .
2. En la ventana "Exportar tabla", seleccione las columnas que quiere exportar. Tiene la opción



de exportar la página actual o las filas seleccionadas.


Export table ×

Columns to export (6)

- Weakness Name
- Description
- Severity
- Impacted Assets
- sources
- Last Seen

+ Add more columns

Current page
 Selected rows

Cancel × Export 

3. Haga clic en **Exportar**.

Personalizar columnas

Puede agregar, quitar o reordenar columnas para adaptar la vista a sus preferencias. Si quiere revertir algún cambio, puede restablecer la configuración predeterminada en cualquier momento.

Para personalizar la visualización de las columnas:

1. En el encabezado de la página **Información general sobre la exposición**, haga clic en .

Aparece la ventana “Personalizar columnas”.

Reorder added columns	Show / Hide	Remove
1. Weakness Name	<input checked="" type="checkbox"/>	-
2. Description	<input checked="" type="checkbox"/>	-
3. Severity	<input checked="" type="checkbox"/>	-
4. Impacted Assets	<input checked="" type="checkbox"/>	-
5. Sources	<input checked="" type="checkbox"/>	-
6. Last Seen	<input checked="" type="checkbox"/>	-

+ Add columns

Reset to defaults × Cancel Apply columns

2. Opcional:

- En la sección **Reordenar las columnas agregadas**, haga clic en el nombre de una columna y arrástrelo para reordenar las columnas.
- En la sección **Mostrar/Ocultar**, seleccione las casillas o anule la selección para mostrar u ocultar las columnas en la tabla.
- En la sección **Quitar**, haga clic en (-) para quitar de manera permanente una columna de la tabla.
- Para agregar columnas a la tabla, haga clic en **Agregar columnas**.

Aparece la ventana **Agregar columnas a la tabla**.

- (Opcional) Utilice la barra de búsqueda para buscar una propiedad de una columna. La lista de propiedades de columnas se actualiza según la consulta de búsqueda.
- Seleccione la casilla junto a las columnas que quiera agregar a la tabla.



- Haga clic en **Agregar**.

La columna aparece en la ventana "Personalizar columnas".

3. Haga clic en **Aplicar columnas**.

Tenable guarda los cambios en las columnas de la tabla.

Columnas predeterminadas

El diseño predeterminado de las columnas garantiza que se pueda acceder fácilmente a los datos clave y, al mismo tiempo, ofrece flexibilidad para la personalización.

- **Nombre de la debilidad**
- **Descripción**
- **Gravedad**
- **Activos afectados**
- **Orígenes**
- **Última visualización**

Para restablecer las columnas predeterminadas:

- Haga clic en **Restablecer valores predeterminados** para restablecer todas las columnas a sus valores predeterminados.

Consulte también

- [Instancias de exposición](#)

Instancias de exposición

En la página **Instancias de exposición** se muestra una lista de casos específicos de debilidades identificadas.

Para acceder a la página **Instancias de exposición**:

1. En el panel de navegación izquierdo de Tenable Identity Exposure, haga clic en el ícono del Centro de exposición



2. En el submenú, haga clic en **Instancias de exposición**.

Aparece la página **Instancias de exposición**.

Weakness Name ↓	Instance Name ↑	Identity Provider ↑	Active Findings ↑	Severity ↑	Remediation Cost ↑
Privileged Entra Account With Access To M365 Services	Default	Default	3	Medium	Low
Privileged Entra Account Synchronized With AD (Hybrid)	Default	Default	1	High	Medium
Entra Security Defaults Not Enabled	Default	Default	1	Medium	Low

Información general

En esta página se muestra una tabla en la que se indican todas las instancias de exposición, con su información correspondiente:

- **Nombre de la debilidad:** nombre genérico de la debilidad.
- **Nombre de la instancia:** nombre específico de esta instancia.
- **Proveedor de identidad:** nombre del proveedor de identidad donde se originaron los datos.
- **Cantidad de hallazgos activos.**
- **Gravedad:** criticidad de esta debilidad.
- **Costo de corrección:** esfuerzo necesario para abordar esta debilidad (bajo, medio, alto).

Información detallada

- Para obtener más detalles sobre cada instancia de exposición, haga clic en la flecha al final de la línea. De esta forma, se abre otra página con la siguiente información para cada instancia

de exposición:

Exposure Instances

[Back to Exposure Instances](#)

EXPOSURE INSTANCE

Unverified Domain / Default

Misconfiguration | Low | [Hide Summary](#)

Weaknesses
Entra ID requires to confirm ownership of new custom domains. The unverified state should only be temporary and all domains must be confirmed, or deleted, to keep the list tidy and make reviews easier.

Remediation cost
●●●

Search for an asset name Show Resolved

Impacted Asset ↑	Providers ↑	Class ↑	Tenant ↑	ACR ↑	Status ↑	Last Status Change ↑	
NewDomain.corp		Resource	QA - Light Tenant	0	Open	Sep 27, 2024	→
NewDomain.corp		Resource	QA - Light Tenant	0	Open	Sep 27, 2024	→
unverified.example.net		Resource	t8qdy	0	Open	Sep 26, 2024	→

Items per page: 25 [Previous page](#) 1 [Next page](#) 1-3 of 3

Información del encabezado

En el encabezado se muestra la siguiente información:

- Tipo de debilidad (como un error de configuración) y nombre de la instancia (predeterminado).
- Gravedad: gravedad de la debilidad (baja, media, alta).
- Descripción de la debilidad: explicación detallada de la debilidad y por qué representa un riesgo de seguridad.
- Costo estimado de corrección.

Lista de activos afectados

Los activos afectados son aquellos en los que la instancia de exposición tuvo un impacto, con sus detalles correspondientes:

- Proveedor.
- Tipo de activo.



- Inquilino: el término “inquilino” se utiliza de forma genérica para hacer referencia a los inquilinos del proveedor de identidad (IdP), aunque cada IdP puede tener su nombre específico para este concepto (por ejemplo, inquilino de Entra ID, dominio de AD, etc.).
- Puntuación del Índice de Criticidad del Activo (Asset Criticality Rating, ACR).
- Estado: Abierto, Resuelto o Resurgido.
- Fecha del último cambio de estado.

Analizar los hallazgos

Para ver el hallazgo asociado al activo afectado, haga clic en la flecha al final de la línea. De esta forma, se abre otra página con esta información para el hallazgo:

Exposure Instances

FINDING

QA - Light Tenant

Unrestricted Guest Accounts / Default

Medium RESOURCE 1 PROVIDER Hide Summary

About this risk

By default, while guest users in Entra ID have limited access to reduce their visibility within the tenant, it is also possible to enhance security and privacy by further tightening these restrictions.

About this asset

The asset QA - Light Tenant is a TENANT type of asset. It is a part of AzureAD.

Finding Status: **Open**

Asset Criticality Rating: 0/10 Tenable Provided

Remediation Cost: **Medium**

MITRE ATT&CK Information: T1078.001, T1078.004, T1590 (+2)

Asset details Weakness details Remediate

Key Properties

Asset Class	Resource	Created Date	Sep 27, 2024 at 08:53 am
Last Observed At	Sep 27, 2024 at 08:53 am		

Asset Information (31) Show More

Algorithm Class	ALL	Asset ID	82270205-6d31-5ba0-b2d1-3374961892bb
-----------------	-----	----------	--------------------------------------

Información del encabezado

En el encabezado de la página **Hallazgo** se muestra la siguiente información:



- **Nombre del inquilino.**
- **Nombre de la debilidad** y nombre de la instancia de exposición asociada.
- **Gravedad:** gravedad de la debilidad (baja, media, alta).
- **Clase de activo:** categoría a la que pertenece el activo. Consulte [Asset Classes](#) (Clases de activos) para obtener más información.
- **Proveedor:** proveedor de identidad.
- **Resumen** de la instancia de exposición:
 - En “Acerca de este riesgo” se ofrece una breve descripción de esta debilidad.
 - En “Acerca de este activo” se indica el tipo de activo (por ejemplo, “inquilino”) y el proveedor de identidad.

Estados de los hallazgos

Los hallazgos pueden mostrar los siguientes estados:

Nota: De forma predeterminada, en la página solo se muestran los hallazgos abiertos y resurgidos.

- **Abierto:** indica un problema de seguridad activo que necesita atención. La debilidad se detectó y aún no se corrigió.
- **Resuelto:** este estado muestra que la debilidad identificada previamente se corrigió correctamente. El problema de seguridad ya no está activo.

Sugerencia: Habilite el conmutador “Mostrar resueltos” para mostrar los hallazgos resueltos.

- **Resurgido:** este estado aparece cuando se vuelve a detectar un problema resuelto previamente. Puede indicar que la solución fue temporal o que el problema volvió a aparecer.

Índice de Criticidad del Activo (Asset Criticality Rating, ACR)

Tenable asigna un valor de ACR a cada activo de su proveedor de identidad para representar la criticidad relativa del activo como un número entero del 1 al 10. Un valor de ACR más alto indica una mayor criticidad. Consulte [ACR](#) para obtener más información.



Costo de corrección

El costo de corrección se refiere al esfuerzo estimado necesario para corregir una debilidad específica, teniendo en cuenta una combinación de trabajo humano, complejidad y posibles gastos financieros.

Se representa en tres niveles:

- Bajo: relativamente fácil de reparar, requiere un tiempo y unos recursos mínimos.
- Medio: requiere un esfuerzo de corrección moderado.
- Alto: problemas complejos que pueden requerir mucho tiempo, muchos recursos o muchos cambios para resolverse.

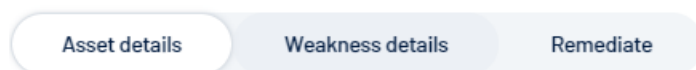
Esta clasificación ayuda a priorizar qué problemas abordar primero en función de su gravedad y del esfuerzo necesario para repararlos.

Información de MITRE ATT&CK

Técnicas relacionadas del [marco MITRE ATT&CK](#).

Detalles de los hallazgos

Debajo del encabezado, en la página “Hallazgos” se muestran tres pestañas para destacar la siguiente información:



- Haga clic en cualquiera de estas pestañas para ampliar los detalles.

Detalles del activo

“Detalles del activo” es la pestaña que está abierta de forma predeterminada en la página “Hallazgos”.



Asset details Weakness details Remediate

Key Properties

Asset Class	Resource	Created Date	Sep 27, 2024 at 08:53 am
Last Observed At	Sep 27, 2024 at 08:53 am		

Asset Information (31) [Show More](#)

Algorithm Class	ALL	Asset ID	82270205-6d31-5ba0-b2d1-3374961892bb
Asset Name	NewDomain.corp	Asset Type	RESOURCE
Cloud Entitlement Properties Dict	Show More	Entra ID Tenant Name	QA - Light Tenant

asset_type	DOMAIN
authentication_type	Managed

En esta sección se proporciona la siguiente información:

- **Propiedades clave:** en esta sección se proporcionan detalles generales sobre el activo, como la clase de activo. También se muestran la fecha de creación del activo y la fecha de la última observación.
- **Información del activo:** esta sección contiene atributos más detallados del activo relacionados con la información del proveedor de identidad.

Detalles de la debilidad

Asset details Weakness details Remediate

Weakness description

[B2B collaboration](#) is a Microsoft Entra ID feature that allows your users to invite guests to collaborate with your organization. These guest users, also called "external identities", by default get access as [described by Microsoft](#):

They can manage their own profile, change their own password, and retrieve certain information about other users, groups, and applications. However, they cannot read all directory information. For example, guest users cannot enumerate the list of all users, groups, and other directory objects. It is possible to add guests to administrator roles, granting them full read and write permissions. Guests can also invite other guests.

If your organization places a high premium on security and privacy when it comes to guest users, you can enhance these aspects by adjusting the default setting by selecting the ["Guest user access is restricted to properties and memberships of their own directory objects \(most restrictive\)"](#) option that has the following impact:

By default, this setting limits guest access exclusively to their own user profile. This means that even when searching by user principal name, object ID, or display name, guests cannot obtain access to other users. Furthermore, this configuration also restricts access to group information, including group memberships.

Why it matters

Guest users are unrestricted because the authentication policy's [guestUserRoleID](#) is not [2af84b1e-32c8-42b7-82bc-daa82484823b](#) (corresponding to the "Restricted Guest User" role).

En esta sección se proporciona la siguiente información:

Descripción de la debilidad: en términos simples, en esta sección se explica por qué la debilidad puede representar riesgos de seguridad para ayudarlo a comprenderla y corregirla.



Por qué es importante: en esta sección se identifica el caso específico de esta debilidad para que pueda concentrar sus esfuerzos en corregirla.

Corrección

Remediation

To restrict the visibility of guest users within your tenant, you must [restrict guest user access](#) in Entra ID by selecting this option: "Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)".

Bear in mind that this may make collaboration with external users more difficult.

Remediate

Remediation script

```
1 Connect-MgGraph -Scopes 'Policy.ReadWrite.Authorization'
2
3 # Apply "Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)"
4 Update-MgPolicyAuthorizationPolicy -GuestUserRoleId '2af84b1e-32c8-42b7-82bc-daa82484023b'
5
```

En esta sección se explica el proceso de corrección de una debilidad.

Pautas de corrección: en las pautas textuales se proporcionan instrucciones detalladas sobre cómo corregir la debilidad identificada. Estas pautas suelen incluir lo siguiente:

- Instrucciones detalladas sobre cómo corregir la debilidad.
- Prácticas recomendadas para evitar problemas similares en el futuro.
- Vínculos a documentación pertinente o recursos adicionales.

Scripts de corrección: para algunos hallazgos, es posible que estén disponibles scripts de corrección automatizados.

Nota: Es posible que un script no esté disponible debido a la incapacidad del producto para automatizar la corrección. Esto también podría implicar la implementación de cambios organizativos en lugar de una reparación técnica directa. En este caso, verá un mensaje en el que se indica que solo es posible la corrección manual de este hallazgo y que debe seguir las pautas textuales.

Antes de ejecutar el script:

- Revise el contenido para comprender qué cambios realizará.
- Adáptelo a su entorno si es necesario.
- Pruebe el script en un entorno que no sea de producción si es posible.
- Asegúrese de tener los permisos necesarios para ejecutar el script.

Sugerencia: Si bien los scripts de corrección pueden ahorrar tiempo, tenga siempre cuidado y asegúrese de comprender las implicaciones de cualquier cambio automatizado en su entorno.



Para ejecutar el script de corrección:

Puede abrir una consola de PowerShell, pegar el script de corrección y ejecutarlo directamente o, si lo prefiere, descargarlo como un archivo .ps1 para ejecutarlo.

1. Busque el botón “Descargar script” en la pestaña “Corrección”.
2. Haga clic en este botón para descargar el script de corrección.
3. Ejecute el archivo como cualquier script de PowerShell.

Opciones de búsqueda, filtrado y exportación

Buscar

- En la lista de instancias de exposición, puede buscar una instancia específica por **nombre de debilidad, nombre de instancia o gravedad**.
- En el cuadro “Buscar”, escriba un término de búsqueda (por ejemplo, “Entra”). En la lista se muestran todas las instancias que coinciden con los criterios de búsqueda.

Weakness Name ↓	Instance Name ↑	Active Findings ↑	Severity ↑	Cost ↑
Single Member Entra Group	Default	38	Low	... →
Privileged Entra Account With Access To M365 Services	Default	5	Medium	... →
Privileged Entra Account Synchronized With AD (Hybrid)	Default	4	High	... →
Empty Entra Group	Default	42	Low	... →

- En la instancia de exposición, puede buscar activos afectados específicos.
- En el cuadro “Buscar”, escriba el **nombre de un activo** (por ejemplo, “Seguridad”). En la lista se muestran todas las instancias que coinciden con los criterios de búsqueda.

Impacted Asset ↓	Providers ↑	Class ↑	Tenant ↑	ACR ↑	Status ↑	Last Status Change ↑
Security Readers	...	Group	t8qdy	0	Open	Aug 28, 2024 →
Security Readers	...	Group	t8qdy	0	Open	Aug 28, 2024 →

Filtrar



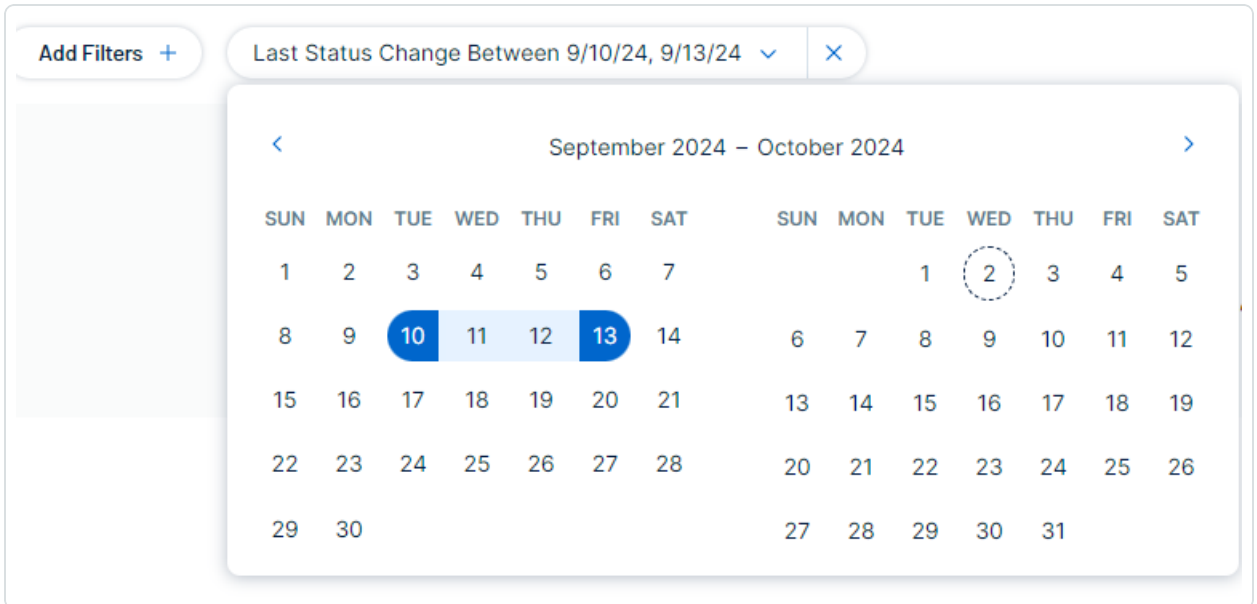
Para filtrar la lista de debilidades:

1. Haga clic en el ícono .

Aparece el botón “Agregar filtro”.

2. Haga clic en “Agregar filtro”. Tiene estas opciones de filtros:

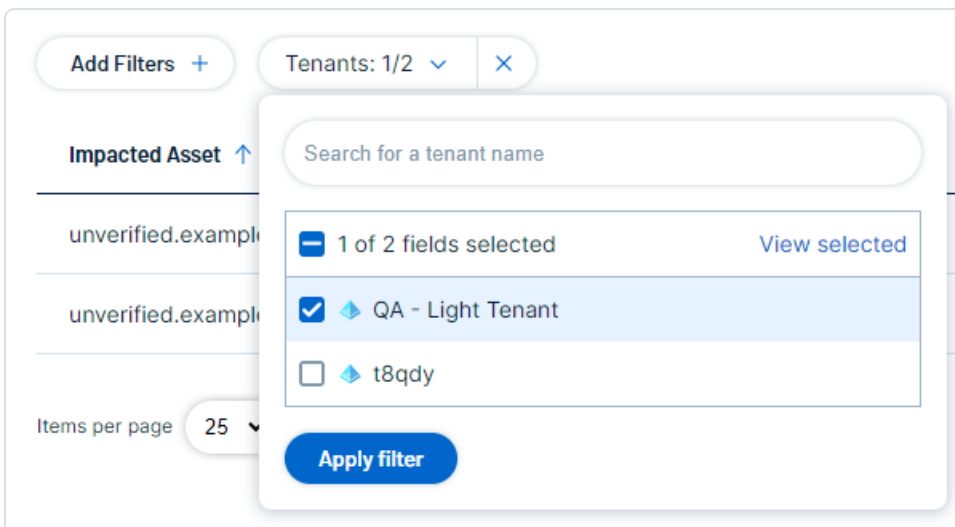
- Por “Último cambio de estado”: seleccione una fecha en el selector de fechas.



The screenshot shows a filter interface with the following elements:

- Add Filters +** button
- Filter label: **Last Status Change Between 9/10/24, 9/13/24** with a dropdown arrow and a close button (X).
- Calendar view for **September 2024 – October 2024**.
- Calendar grid with days of the week (SUN to SAT) and dates. The dates **10** and **13** are highlighted in blue.

- Por “Inquilino”: seleccione el nombre del inquilino. También puede buscar un inquilino específico en el cuadro “Buscar” y hacer clic en **Ver seleccionados**.



The screenshot shows a filter interface with the following elements:

- Add Filters +** button
- Filter label: **Tenants: 1/2** with a dropdown arrow and a close button (X).
- Impacted Asset** section with a search box labeled **Search for a tenant name**.
- Search results list:
 - 1 of 2 fields selected View selected
 - QA - Light Tenant
 - t8qdy
- Items per page** dropdown set to 25.
- Apply filter** button.



3. Haga clic en **Aplicar filtro**.

Exportar

Puede exportar la lista de activos afectados de una instancia de exposición como un archivo de Excel.

Para exportar:

- En la página de instancia de exposición, haga clic en el ícono .

Consulte también

- [Información general sobre la exposición](#)

Identidad 360: gestión integral de riesgos de identidad

Identidad 360 es una nueva funcionalidad de Tenable Identity Exposure centrada en la identidad, que ofrece un inventario completo y exhaustivo de cada identidad en la superficie de riesgo de identidades de la organización.

Esta funcionalidad unifica las identidades de Active Directory y Entra ID y permite clasificarlas según su riesgo, de modo que pueda clasificar las identidades en su organización desde la de mayor riesgo a la de menor.

Además, **Identidad 360** permite a los usuarios comprender de manera cabal cada identidad a través de diversas perspectivas contextuales, como cuentas, debilidades y dispositivos asociados con una identidad determinada para obtener una visión completa de esa identidad.

Funcionalidades clave

- **Vista de identidades unificada:** Identidad 360 agrupa las identidades de varios proveedores de identidad, comenzando con Active Directory y Entra ID.
- **Clasificación basada en riesgos:** al aprovechar el análisis avanzado, Identidad 360 le permite clasificar las identidades de su organización desde la de mayor riesgo a la de menor. Esta priorización permite a los equipos de seguridad concentrar sus esfuerzos donde más



importan, lo que optimiza la asignación de recursos y mejora la posición de seguridad general.

- **Información de identidad contextual:** obtenga una comprensión cabal de cada identidad a través de varias perspectivas contextuales:
 - Cuentas asociadas
 - Debilidades identificadas
 - Dispositivos conectados
 - Privilegios de acceso
 - Patrones de actividad

Este enfoque multifacético brinda una perspectiva completa de cada identidad, lo que permite realizar evaluaciones de riesgos más precisas y adoptar medidas de seguridad específicas.

- **Inteligencia procesable:** al consolidar información de las identidades de distintos orígenes, Identidad 360 ofrece información procesable que permite a los equipos de seguridad:
 - Identificar y corregir vulnerabilidades asociadas a identidades de alto riesgo.
 - Implementar políticas más eficaces de control de acceso.
 - Detectar posibles amenazas internas y responder a ellas más rápidamente.
 - Optimizar los informes y las auditorías de cumplimiento.

Al centralizar la gestión del riesgo de identidad y dar una visión holística del panorama de identidades de su organización, **Identidad 360** ayuda a reducir la superficie de ataque, mejorar la eficiencia operativa y fortalecer la posición de seguridad general.

¿Qué es una identidad?

Una **identidad** es la representación digital de un ser humano (o no humano).

- Quién es (nombre, puesto, departamento, etc.).
- A qué puede acceder (archivos, sistemas, datos).
- Cómo interactúa con el mundo digital de la organización.



Por otro lado, una **cuenta** es solo una parte de una identidad. Es como una llave que permite a la persona iniciar sesión en un sistema o servicio en particular. Por ejemplo, alguien puede tener una cuenta de correo electrónico laboral, una cuenta de base de datos de clientes y una cuenta de una herramienta de gestión de proyectos: todas ellas son distintas partes de su identidad digital general.

Al analizar la identidad como un todo en lugar de solo las cuentas individuales, Identidad 360 le brinda una imagen más completa de la presencia digital y los riesgos potenciales de cada persona.

Datos de Identidad 360

Identidad 360 aprovecha los datos de la plataforma Tenable, lo que proporciona a Tenable Identity Exposure un acceso sin precedentes a los datos para evaluar la posición de seguridad de su organización.

En el ecosistema de Tenable, las entidades se denominan "activos". Tenable Identity Exposure continúa destacando las vulnerabilidades asociadas a estos activos y, a la vez, revela sus relaciones a través de páginas de activos detalladas.

Nota: Al visualizar las propiedades de los activos, algunos campos pueden mostrar mayúsculas y minúsculas incorrectas (por ejemplo, minúsculas) en comparación con su formato original en el proveedor de identidad (IdP).

Nota: La funcionalidad Información general sobre la exposición actualmente muestra datos relacionados con debilidades según el **perfil predeterminado de Tenable** y no refleja automáticamente el **estado de las anomalías en los objetos de AD que se permitieron en otros perfiles**.

Por lo tanto:

- Si **permitió un objeto de AD** para un indicador de exposición en particular (por ejemplo, "Miembro de grupos administrativos nativos"), **Información general sobre la exposición aún lo marcará como una debilidad de seguridad si el perfil predeterminado lo identificó como anómalo**.
- Esto puede generar la impresión de que el problema no se ha abordado, aunque el objeto ya se haya permitido con otro perfil.
- Si se adopta una medida correctiva (como eliminar la membresía al grupo) según lo que se ve en Información general sobre la exposición, el objeto desaparecerá de la vista, pero esto podría no haber sido necesario si el objeto ya se hubiera permitido en otro lugar.



Recopilación de identidades

Identidad 360 consolida las cuentas del IdP bajo una entidad unificada de tipo Persona. Para determinar si debe asociar cuentas, **Identidad 360** compara varios atributos, como las direcciones de correo electrónico de las cuentas y los nombres principales de usuario (UPN).

Tenable prioriza las coincidencias de alta calidad para evitar asociaciones erróneas, incluso si eso significa perder ocasionalmente coincidencias que parecen obvias para un observador humano. Por ejemplo, Tenable excluye los nombres y los apellidos de las coincidencias porque la alta probabilidad de homónimos en organizaciones grandes aumenta significativamente el riesgo de falsos positivos.

Nota: Cuando el IdP elimina la última cuenta asociada a una persona, la interfaz de usuario de Tenable Identity Exposure puede tardar hasta 12 horas en eliminar el activo de persona correspondiente. **Identidad 360** también puede mostrar relaciones duplicadas entre una persona y sus cuentas asociadas.

Inquilino, dominio y organización del IdP

Tenable utiliza el término “inquilino” para abarcar varios conceptos del IdP, tales como “inquilino” (por ejemplo, en Microsoft Entra ID), “organización” (por ejemplo, en Okta) y “dominio” (por ejemplo, en Microsoft Active Directory).

Para obtener más información sobre cómo Tenable identifica a los inquilinos de los objetos del IdP, consulte [Descripción de la pertenencia a inquilinos](#).

Activos y orígenes de datos entre productos

Identidad 360 ofrece una vista integral de todos los datos relacionados con la identidad en el ecosistema de Tenable. Esto incluye datos de Tenable Identity Exposure, datos de seguridad en la nube e, incluso, resultados de escaneos de Nessus. El producto específico de Tenable que recopila cada conjunto de datos se denomina “origen”.



	Name	Sources	Provider Names	AES	Weaknesses	Accessible Reso...
<input type="checkbox"/>	Administrator			915	2	216
<input type="checkbox"/>	Administrator			905	4	742
<input type="checkbox"/>	dcadmin	 		905	4	12
<input type="checkbox"/>	Administrator			893	0	3218

Otro detalle clave es el tipo de datos disponibles, como los nombres de IdP, como Active Directory, Entra ID y AWS. Esta información aparece en la columna "Nombre de proveedores". Los campos "Origen" y "Nombre de proveedores" admiten filtrado y clasificación, y cada uno puede contener varios valores.

Datos entre productos (orígenes de datos)

Identidad 360 muestra todos los datos orientados a la identidad disponibles en el ecosistema de Tenable. Un activo determinado puede tener uno o varios orígenes; es decir, uno o varios productos de Tenable pueden observarlo. Tenable Identity Exposure presenta datos recopilados del propio Tenable Identity Exposure, así como de orígenes complementarios.

The screenshot shows the Tenable Identity Exposure interface. At the top, it says "tenable Identity Exposure". Below that, it shows "Identities" and a "Back to Identities" button. The main content area displays details for a "PERSON" named "dcadmin". A red box highlights the "Sources" section, which lists: "Tenable Vulnerability Management", "Tenable Identity Exposure (AD)", "Tenable Identity Exposure (Entra ID)", and "No summary generated yet". Below this, there are three summary cards: "Asset Exposure Score" (905/1000), "Asset Criticality Rating" (10/10), and "Weaknesses Identified" (4, with a note "Coming from 1 account"). To the right, there is a "Key Properties" section with fields for "Owner", "Location", and "Last Update" (29 janv. 2025 at 19:07). At the bottom, there is a navigation bar with tabs for "Properties", "Accounts", "Devices", "Weaknesses", "Entitlements", "Roles", "Groups", "Access", "Exposure Cards", and "Relationships". A search bar is also visible at the bottom left.

Los posibles orígenes incluyen:

Licencia necesaria	Requisitos previos de configuración	Orígenes de activos	Valor
--------------------	-------------------------------------	---------------------	-------



Tenable Identity Exposure o Tenable One	<ul style="list-style-type: none">• Un dominio de Active Directory (AD) en Tenable Identity Exposure.• Datos enviados a la plataforma en la nube de Tenable.	Tenable Identity Exposure (AD)	Datos completos de AD
Tenable Identity Exposure o Tenable One	<ul style="list-style-type: none">• Un inquilino de Microsoft Entra ID (MEID) en Tenable Identity Exposure.	Tenable Identity Exposure MEID	Datos completos de MEID
Tenable One	<ul style="list-style-type: none">• Un proveedor de identidad en Tenable en Tenable Cloud Security.	Tenable Cloud Security	Datos de IdP adicionales en ID360: AWS, Okta, GCI, OneLogin y PingIdentity. Los datos se restringirán a las cuentas de IdP que tengan direcciones de correo electrónico completadas en el IdP.
Tenable One	<ul style="list-style-type: none">• Un escaneo de Nessus que aproveche el complemento 171956: Windows Enumerate Accounts (Enumeración de cuentas de Windows). Para obtener más detalles sobre los escaneos, consulte Scans	Tenable Vulnerability Management	Asignación entre cuentas de Active Directory (AD) y Entra ID, junto con los dispositivos que



	<p>Overview (Información general de escaneos) en Tenable Vulnerability Management User Guide (Guía del usuario de Tenable Vulnerability Management).</p>		usan estas cuentas.
--	--	--	---------------------

Requisitos previos

Para usar **Identidad 360**, tiene que activar la compatibilidad con Identidad 360 en la configuración de Tenable Identity Exposure.

- (Opcional) Para enviar los datos de Active Directory para su análisis, también tiene que activar el servicio de Tenable Cloud.

tenable Identity Exposure

Configuración del sistema

Gestión de retransmisiones Gestión de bosques Gestión de dominios Gestión de inquilinos Configuración Acerca de Información legal

SERVICIOS DE APLICACIÓN

- > Servidor SMTP
- > Registros de actividad
- > Entidades de certificación de confianza
- > Indicadores de ataque
- > **Tenable Cloud**
- > Retransmisión
- > Verificación de estado

MOTOR DE ALERTAS

- > SYSLOG
- > Correo electrónico

INFORMES

- > Centro de informes

AUTENTICACIÓN

- > Tenable one

Activar compatibilidad de Identidad 360 con el Centro de exposición y Microsoft Entra ID

Tenable Identity Exposure usa el servicio de Tenable Cloud para admitir la compatibilidad de Identidad 360 con el Centro de exposición y Microsoft Entra ID.

Al habilitar esta característica, Tenable Identity Exposure recuperará los datos de Tenable Cloud y comenzará el análisis de seguridad de los inquilinos de Microsoft Entra ID. Esta característica no transfiere los datos de AD a Tenable Cloud.

Para activar esta característica, se necesita una conexión entre Tenable Identity Exposure y el servicio de Tenable Cloud a través del registro de la clave de API. Para ello, ingrese su clave de acceso y clave secreta o vaya al [portal de Tenable Cloud](#) para generarlas.

En funcionamiento

Usar el servicio de Tenable Cloud

Cuando se activa el servicio de Tenable Cloud, Tenable Identity Exposure transfiere la información que recopila a la nube privada de Tenable para brindarle más análisis de seguridad innovadores y nuevos servicios avanzados, en especial cuando usa otros productos de Tenable, entre otros.

Dado que la seguridad y la transparencia son fundamentales para nuestros valores corporativos, consulte nuestra declaración de [Confianza y seguridad](#) para obtener más información sobre cómo gestionamos los datos que recopilamos de usted.

Al activar esta opción, indica que Tenable Identity Exposure también puede transferir a la nube privada de Tenable los datos que recopila a través del "análisis con privilegios" (cuando se configuró en sus dominios). Si no activa este servicio, Tenable no puede llevar a cabo ciertos análisis.

En funcionamiento

Configuración

- Configuración del sistema
- Gestión de bosques
- Gestión de dominios
- Información de la licencia
- Gestión de usuarios
- Gestión de roles
- Configuración de perfiles
- Registros de actividad

Precaución: Para utilizar esta funcionalidad, **no debe** aplicar el filtrado de direcciones IP en Tenable Vulnerability Management para permitir el acceso de la API a Tenable Identity Exposure. Consulte [API Access Security](#) (Seguridad de acceso a la API) para obtener más información.

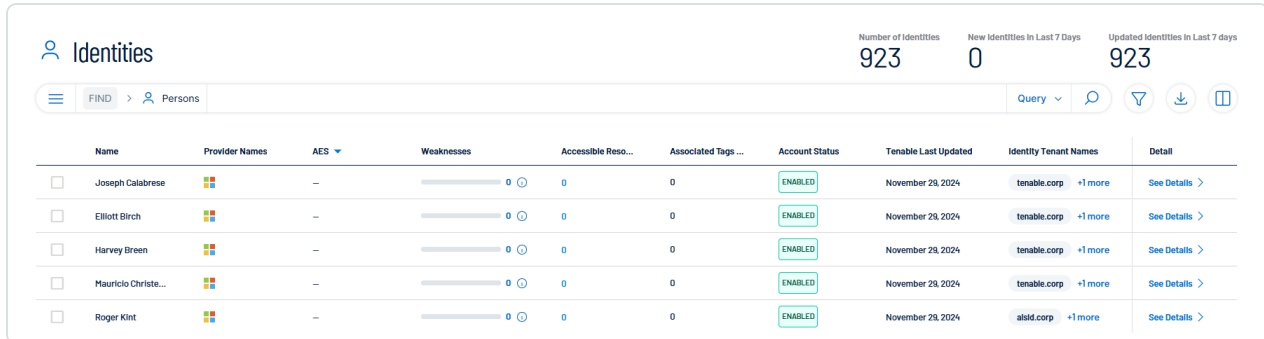












Acceder a “Información general de identidades”

Para abrir la página **Información general de identidades**:

- En Tenable Identity Exposure, haga clic en  en la barra de navegación de la izquierda.

La página **Información general de identidades** se abre con un tablero de control para gestionar y supervisar las identidades dentro del sistema de una organización.



Name	Provider Names	AES	Weaknesses	Accessible Reso...	Associated Tags ...	Account Status	Tenable Last Updated	Identity Tenant Names	Detail
<input type="checkbox"/> Joseph Calabrese		-	 0 0	0	0	ENABLED	November 29, 2024	tenable.corp +1 more	See Details >
<input type="checkbox"/> Elliott Birch		-	 0 0	0	0	ENABLED	November 29, 2024	tenable.corp +1 more	See Details >
<input type="checkbox"/> Harvey Green		-	 0 0	0	0	ENABLED	November 29, 2024	tenable.corp +1 more	See Details >
<input type="checkbox"/> Mauricio Christie...		-	 0 0	0	0	ENABLED	November 29, 2024	tenable.corp +1 more	See Details >
<input type="checkbox"/> Roger Kint		-	 0 0	0	0	ENABLED	November 29, 2024	atsid.corp +1 more	See Details >

Elementos principales

Este tablero de control le permite ver, buscar y gestionar información de las identidades, con un foco puesto en las métricas de seguridad, como debilidades y exposición a ataques. Allí encontrará una descripción general (en el encabezado) e información detallada sobre las identidades individuales en formato de tabla.

- **Métricas clave**

- Cantidad de identidades
- Identidades nuevas en los últimos 7 días
- Identidades actualizadas en los últimos 7 días

- **Navegación y búsqueda**

- Barra de búsqueda para consultar identidades.
- Opciones para consultas, filtros, exportaciones y personalización de columnas.



Para obtener información completa sobre cómo usar la función de búsqueda, consulte [Global Search Quick Reference Guide](#) (Guía de referencia rápida de búsqueda global).

- **Tabla de datos** de todos los activos de identidad de los proveedores de identidad (IdP). Esta vista se centra específicamente en los activos del tipo de identidad, a diferencia de Tenable One, que muestra todos los tipos de activos. Cada fila representa una identidad única con esta información: (visualización de columnas predeterminada).
 - Nombre, Proveedores, AES (Asset Exposure Score), Debilidades, Recursos accesibles, Etiquetas asociadas, Estado de la cuenta, Última actualización, Nombres de inquilinos de identidades y Detalles.
- **Visualización de datos**
 - Gráficos de barras o indicadores en las columnas “AES” y “Debilidades”, que muestran una representación visual de los datos.
- **Indicadores de estado**
 - Etiqueta “HABILITADA/DESHABILITADA” en la columna Estado de la cuenta.

Comparación con Tenable One Inventory

La interfaz de **Identidad 360** tiene una apariencia y funcionalidad similares a Tenable One Inventory, con adaptaciones específicas para la gestión de identidades. El diseño y muchas funcionalidades le resultarán familiares si ya utiliza Tenable One.

Para obtener más información, consulte [Tenable One Exposure Management Platform Deployment Guide](#) (Guía de implementación de la Plataforma de gestión de exposición Tenable One).

Consulte también

- [Descripción de la pertenencia a inquilinos](#)

Detalles de identidad

La página **Detalles de identidad** se centra en una identidad individual y brinda una vista integral de la huella digital, los derechos de acceso, las posibles vulnerabilidades y la posición de seguridad general de una identidad dentro del ecosistema de TI de una organización.

Para acceder a esta página:



- En la página **Información general de identidades**, haga clic en **Ver detalles** al final de la fila que contiene el nombre de la persona en la tabla.

PERSON

Joseph Calabrese

Source: [Tenable Identity Exposure \(AD\)](#) | [Hide Summary](#) ^

About this asset
Joseph Calabrese is an identity asset associated with LDAP. It is a critical asset for the organization as it represents an individual user with access to various systems and resources. The asset has a medium relative exposure, indicating that it is moderately vulnerable to attacks. One highlighted weakness is the lack of multi-factor authentication (MFA), which increases the risk of unauthorized access to the account.

Weaknesses
The asset doesn't have any weaknesses

Asset Exposure Score
285/1000

Asset Criticality Rating
2/10

Weaknesses Identified
0
Coming from 2 accounts

Key Properties
Owner: -
Location: -
Last Update: Nov 29, 202...

Properties Accounts Devices Weaknesses Entitlements Roles Groups Access ...

Search...

Key Properties

Asset Class	Person	Tenable Created Date	Oct 24, 2024 at 02:17 am
Tenable Last Observation Date	Nov 29, 2024 at 12:21 pm		

Asset Information (34) [Show More](#)

AD Domain Name	tenable.corp alsid.corp	Accessible Resources	0
Account Status	Enabled	Asset ID	00026198-4ea5-47ac-ac72-e6f0e5c6a8d8
Associated Tags Count	0	Exposure Classes	IDENTITY
First Name	Joseph	Identity License Status	Never expires
Identity Tenant Names	tenable.corp alsid.corp		

Encabezado y sección superior

- **Nombre de la identidad:** muestra el nombre de la identidad.
- **Ícono de persona y Origen:** muestran la asociación de la identidad con orígenes específicos. Al pasar el cursor por los íconos de origen, aparecerá el nombre del proveedor de identidad.
- **Resumen:** muestra un resumen detallado sobre la identidad y las debilidades detectadas para esta identidad.


Generar y ver un resumen de IA del activo

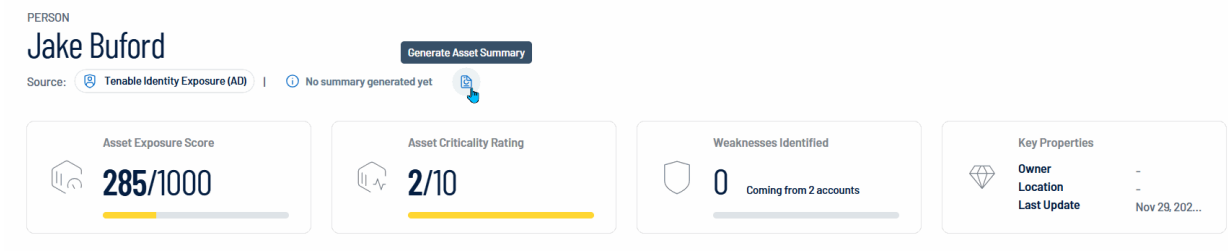





Tenable Identity Exposure le permite generar un resumen de una identidad con IA. Los resúmenes se generan en el nivel de contenedor y solo se aplican a las identidades con licencia de su contenedor.

Nota: Tenable Identity Exposure limita la cantidad de resúmenes que puede generar a 100 por hora, con un máximo de 1000 resúmenes por día.

Siga uno de los procedimientos a continuación:

- Si quiere generar un resumen de IA para el activo por primera vez, al lado de **Aún no se generó ningún resumen**, haga clic en el botón .




PERSON
Jake Buford
Source:  Tenable Identity Exposure (AD) |  No summary generated yet 




Generate Asset Summary

Asset Exposure Score 285/1000	Asset Criticality Rating 2/10	Weaknesses Identified 0 Coming from 2 accounts	Key Properties Owner - Location - Last Update Nov 29, 202...
---	---	---	--

Tenable Identity Exposure utiliza la IA para generar un resumen del activo que incluye detalles generales y específicos sobre las debilidades de dicho activo.

- Si quiere volver a generar un resumen de IA existente para el activo, haga clic en **Mostrar resumen** y, en la parte inferior del panel de resumen, haga clic en el botón .

Tenable Identity Exposure vuelve a generar el resumen de IA para la identidad.

Sugerencia: Haga clic en el botón  para copiar el resumen directamente en su portapapeles. Para calificar la utilidad del resumen, haga clic en  o  y, así, ayudará a mejorar la calidad del contenido generado por IA en Tenable Identity Exposure en el futuro.

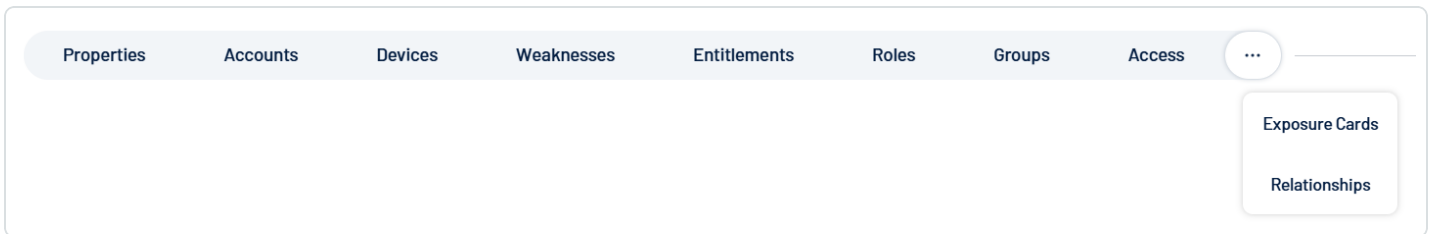
- **Asset Exposure Score:** cuantifica la exposición de seguridad de la identidad, donde una puntuación máxima de 1000 representa el nivel más alto de exposición.
- **Asset Criticality Rating:** refleja la importancia de la identidad dentro de la organización, calificada en una escala del 1 al 10, donde 10 representa la mayor criticidad.
- **Debilidades identificadas:** muestra la cantidad de debilidades o vulnerabilidades de seguridad identificadas para esta identidad específica.



- **Propiedades clave:** enumera información clave, incluido el propietario, la ubicación y la fecha de la última actualización de esta identidad.

Pestañas de encabezado

Debajo del encabezado, las pestañas específicas ofrecen información detallada específica de la categoría. Consulte las descripciones detalladas de cada pestaña en la sección a continuación.



- **Propiedades:** información básica y atributos de la identidad.
- **Cuentas:** cuenta asociada y perfil de red de la identidad.
- **Dispositivos:** dispositivos electrónicos asociados a la identidad.
- **Debilidades:** vulnerabilidades o riesgos de seguridad específicos.
- **Derechos:** permisos o derecho de acceso específicos que se otorga a una identidad dentro de los sistemas de TI de una organización.
- **Roles:** conjunto de derechos agrupados según puestos laborales, responsabilidades o cargos en la organización.
- **Grupos:** unidades organizativas o equipos a los que pertenece la identidad.
- **Acceso:** descripción general de a qué recursos o sistemas puede acceder esta identidad.
- **Tarjetas de exposiciones:** resúmenes de los niveles de exposición al riesgo.
- **Relaciones:** conexiones con otras identidades o entidades.

Cuando esté disponible, haga clic en “Ver detalles” para ver más detalles en [Tenable Inventory](#).

Propiedades

En la vista predeterminada se muestra la pestaña “Propiedades”.



Properties Accounts Devices Tags Attack Paths Weaknesses Entitlements Roles Groups Access Exposure Cards Relationships

Search...

Key Properties

Asset Class	Person	Created Date	Mar 5, 2024 at 01:40 pm
Last Observed At	Sep 10, 2024 at 12:45 pm		

Asset Information (42) [Show More](#)

ACR	9	ACR Method	calculated
AES	902	Account Email	cecil.bagley@absid.corp
Algorithm Class	ALL	Asset ID	1cbb18-2c2f-5df8-95c9-e692059fe630
Asset Name	Cecil Bagley	Asset Type	IDENTITY
Associated Tags Count	8	Critical Vuln Count	8

Propiedades clave

Resumen de los atributos más esenciales relacionados con el activo o la identidad. En general, incluye información general, como la clase de activo, la hora de la última observación y otra información fundamental que ofrece una descripción general rápida del estado de la entidad.

Información del activo

Lista detallada de propiedades específicas asociadas al activo o la identidad. Pueden incluirse identificadores técnicos, como ACR, AES, nombre del activo, correo electrónico o fecha de creación, entre otros. Brinda una visión integral de las características y metadatos relacionados con la entidad.

Cuentas

En la sección "Cuentas" se ofrece información detallada sobre la cuenta asociada y el perfil de red de la identidad.



Properties Accounts Devices Tags Attack Paths Weaknesses Entitlements Roles Groups Access Exposure Cards Relationships

cecil.bagley@alsid.corp

Key Properties

Class
Category
ACCOUNT

Description
Tenable.ad test users that likes the product.

Network and administrator profile

OU
ou=alsid,dc=alsid,dc=corp

Domain
alsid.corp

Forest Name
Alsid Forest

Account Providers

Account AES
902

Last Use
-

Last Location Used
-

Account Activity **ACTIVE**

Weakness

6

7

6

0

● Critical 2

● High 2

● Medium 2

● Low 0

Propiedades clave

Incluye detalles esenciales, como la clase de cuenta (tipo de activo), la categoría (por ejemplo, CUENTA) y una descripción del propósito o el rol de la cuenta. En la sección “Perfil de administrador y red” se resaltan detalles técnicos, como la unidad organizativa (OU), el dominio y el nombre del bosque.

Debilidad

Muestra una representación gráfica de la cantidad de debilidades que se encontraron, categorizadas por gravedad (crítica, alta, media y baja). En el gráfico se proporciona una línea de tendencias que indica la progresión de las debilidades a lo largo del tiempo.

Dispositivos

Un dispositivo suele ser un componente físico o virtual que puede conectarse a una red, comunicarse con otros dispositivos y cumplir funciones o tareas específicas asociadas a la identidad.

Para comenzar a ver los dispositivos de esta persona, use Tenable Vulnerability Management para escanear las máquinas donde inicia sesión.



lucqa-afad-clie

Key Properties

Class

Category
general-purpose

Description
-

Drivers
NESSUS:11936, NESSUS:171410:DYNAMIC_IP

Network and administrator profile

Static IP Assignment
10.200.200.6

OU
-

Domain
alsid.corp

Forest Name
-

Device AES
548

Weakness
14

Critical	1
High	8
Medium	5
Low	0

Last Use
10/04/2024, 07:13:20

User
-

Last Location Used
10.200.200.6

Identities Associated With The Device

Devices Using MFA

Device OS
Microsoft Windows Server 2019 Datacenter 10.0.17763 ACTIVE

En cada mosaico, puede ver la siguiente información del dispositivo:

- **Propiedades clave:**

- **Clase:** clase del activo asociada al dispositivo.
- **Categoría:** categoría asociada al dispositivo, por ejemplo, **propósito general**.



- **Descripción:** si está disponible, descripción del dispositivo.
- **Controladores:** lista de controladores instalados en el dispositivo.
- **Perfil de administrador y red:**
 - **Asignación de IP estática:** dirección IP estática asociada al dispositivo.
 - **Unidad organizativa:** unidad organizativa (OU) asociada al dispositivo.
 - **Dominio:** dominio asociado al dispositivo. Para obtener más información, consulte [Dominios](#) en la *Guía del usuario de Tenable Identity Exposure*.
 - **Nombre del bosque:** nombre del bosque asociado al dispositivo. Para obtener más información, consulte [Bosques](#) en la *Guía del usuario de Tenable Identity Exposure*.
- **AES del dispositivo:** AES general asociado al dispositivo. Para obtener más información, consulte [Tenable Inventory Metrics](#) (Métricas de Tenable Inventory).
- **Debilidad:** representación gráfica de las debilidades del dispositivo. Esta sección incluye un gráfico de líneas y un recuento individual de cada debilidad y su criticidad.

Debilidades

- Una **debilidad** es una instancia que indica vulnerabilidades o brechas de seguridad asociadas a esta identidad o sus cuentas.
- Una **vulnerabilidad** es una debilidad técnica en los productos o sistemas de información que puede explotarse para perturbar o dañar actividades económicas y sociales.
- Un **indicador de exposición** (IoE) es una firma de detección que identifica posibles exposiciones de seguridad relacionadas con la identidad dentro del entorno.
- Una **puntuación del riesgo** es una métrica integral que evalúa los riesgos de identidad en toda la organización, teniendo en cuenta diversos elementos, como debilidades, derechos y otros indicadores relacionados con la seguridad, para ofrecer una evaluación general de las amenazas potenciales.



Weakness Name	Type	Severity	VPR	Impacted Assets	Choke Points	Account	Last Seen	
Not protected against delegation	Misconfiguration	Critical	-	8	-	ⓘ	September 10, 2024	See details >
Privileged AD user account synchronized to Entra ID	Misconfiguration	High	-	6	-	ⓘ	September 10, 2024	See details >
Unprotected Tier-0 user account	Misconfiguration	High	-	6	-	ⓘ	September 10, 2024	See details >
Privileged account never used	Misconfiguration	Medium	-	2	-	ⓘ	September 10, 2024	See details >
Dangerous Primary Group	Misconfiguration	Critical	-	2	-	ⓘ	September 10, 2024	See details >
Missing MFA for Non-Privileged Account	Misconfiguration	Medium	-	1798	-	ⓘ	May 29, 2024	See details >

Sugerencia: Para obtener datos más detallados sobre las debilidades, haga clic en “Ver detalles” para ir a la página [Detalles de la debilidad](#) de Inventory.

Nota: Actualmente, esta página está disponible solo para usuarios con licencias de Tenable One.

El mosaico incluye la siguiente información:

- **Nombre:** vulnerabilidad o debilidad específica identificada.
- **Tipo:** categoría o clasificación de la vulnerabilidad; por ejemplo, “error de configuración”.
- **Gravedad:** mide la criticidad de la debilidad, que va de baja a crítica, lo que condiciona el impacto potencial si se explota.
- **VPR:** es el Índice de Priorización de Vulnerabilidades (Vulnerability Priority Rating), una puntuación o rango que indica la urgencia de abordar la debilidad en función de su explotabilidad y daño potencial. Consulte [Vulnerability Priority Rating](#) (Índice de Priorización de Vulnerabilidades).
- **Activos afectados:** enumera los sistemas, aplicaciones o datos que podrían verse afectados si se explota la debilidad.
- **Puntos de congestión:** áreas potenciales del sistema donde se pueden concentrar los esfuerzos de mitigación para limitar el daño o la propagación de un ataque.
- **Cuenta:** cuenta asociada a la debilidad o vulnerabilidad identificada.
- **Última visualización:** fecha u hora en que se detectó la vulnerabilidad por última vez.

Nota: La funcionalidad Identidad 360 actualmente muestra datos relacionados con debilidades según el **perfil predeterminado de Tenable** y no refleja automáticamente el **estado de las anomalías**



en los objetos de AD que se permitieron en otros perfiles.

Por lo tanto:

- Si **permitió un objeto de AD** para un indicador de exposición en particular (por ejemplo, "Miembro de grupos administrativos nativos"), **Identidad 360 aún lo marcará como una debilidad de seguridad si el perfil predeterminado lo identificó como anómalo.**
- Esto puede generar la impresión de que el problema no se ha abordado, aunque el objeto ya se haya permitido con otro perfil.
- Si se adopta una medida correctiva (como eliminar la membresía al grupo) según lo que se ve en Identidad 360, el objeto desaparecerá de la vista, pero esto podría no haber sido necesario si el objeto ya se hubiera permitido en otro lugar.

Derechos

Un **derecho** es un permiso o derecho de acceso específico que se otorga a una identidad dentro de los sistemas de TI de una organización. Representa el nivel detallado de control de acceso y define exactamente qué medidas puede adoptar una identidad en un recurso en particular.

Entitlements	Severity	Trustees	Accessible resources	Roles	Account	Last Use
ACCESS_ALLOWED/WDS_RIGHT_ACTRL_DS_LIST//	- Undefined	925	1.68K	0	Cecil Bagley	September 9, 2024
ACCESS_ALLOWED/WDS_RIGHT_DS_CONTROL_ACCESS//	- Undefined	7	1.15K	0	Cecil Bagley	September 9, 2024
ACCESS_ALLOWED/WDS_RIGHT_DS_CREATE_CHILD//	- Undefined	925	1.15K	0	Cecil Bagley	September 9, 2024

El mosaico incluye la siguiente información:

- **Derechos:** enumera los permisos o derechos de acceso específicos otorgados a las cuentas, como "ACCESS_ALLOWED" con permisos detallados. Pueden representar permisos dentro de un sistema, como Active Directory.
- **Gravedad:** muestra el nivel de criticidad o riesgo asociado a cada derecho. En este caso, está marcada como "Indefinida", lo que sugiere que no se aplica ninguna categorización de riesgo específica.
- **Administradores:** indica el número de usuarios o cuentas (administradores) a quienes se les otorgaron estos derechos o permisos.



- **Recursos accesibles:** muestra la cantidad de recursos (como archivos, carpetas, sistemas, etc.) a los que se puede acceder a través del derecho otorgado.
- **Roles:** muestra cuántos roles están ligados a este derecho específico.
- **Cuenta:** especifica el usuario o la cuenta que están asociados con estos derechos. Por ejemplo, "Cecil Bagley" aparece como titular de la cuenta para los permisos que se muestran.
- **Último uso:** proporciona la última fecha en que se usaron estos derechos e indica en qué momento la cuenta accedió por última vez a los recursos mediante los permisos específicos.

Roles

Un **rol** es un conjunto de derechos agrupados según puestos laborales, responsabilidades o cargos en la organización. Los roles establecen una forma de administrar los derechos de acceso de manera más eficiente, ya que asignan un conjunto de derechos predefinidos a varios usuarios que comparten puestos laborales similares.

En el mosaico **Roles** se muestran todos los roles asignados a la identidad. Por ejemplo, si esta identidad tiene roles asignados en Microsoft Entra ID, los detalles aparecen aquí.

Roles	Origin	Severity ^	Trustees	Entitlements	Last Use
Azure AD Joined Device Local Administrator		Medium	9	2	30 November 2023
User		Medium	951	126	30 November 2023
Global Administrator		Critical	18	195	11 January 2024

El mosaico incluye la siguiente información:

- **Roles:** nombre del rol asignado a la identidad.
- **Origen:** ícono que indica el proveedor de origen de la cuenta.
- **Gravedad:** gravedad general del activo; por ejemplo, **Crítica**.
- **Administradores:** cantidad de administradores asociados al rol de la identidad.
- **Derechos:** cantidad de derechos a los que el rol tiene acceso.
- **Último uso:** fecha en la que se usó el rol por última vez en el activo.



Grupos

Los grupos son unidades colectivas o equipos a los que pertenece esta identidad dentro de la organización.

Group	Account	AES ^	Members	Provider
Domain Admins	Cecil Bagley	-	3	
Domain Users	Cecil Bagley	-	920	

El mosaico incluye la siguiente información:

- **Grupo:** nombre del grupo al que pertenecen los usuarios o las cuentas (por ejemplo, “Administradores de dominio” o “Usuarios del dominio”).
- **Cuenta:** cuenta vinculada a un usuario o entidad específicos (en este caso, “Cecil Bagley”). Podría ser el administrador o el usuario que gestiona el grupo.
- **AES:** Asset Exposure Score. Tenable calcula un AES dinámico para cada activo de la red para representar la exposición relativa del activo como número entero entre el 0 y el 1000. Un valor de AES más alto indica una mayor exposición. Para obtener más información, consulte [Tenable Inventory Metrics](#) (Métricas de Tenable Inventory).
- **Miembros:** cantidad de miembros en cada grupo (por ejemplo, 3 miembros en “Administradores de dominio” y 920 miembros en “Usuarios del dominio”).
- **Proveedor:** proveedor de identidad que es el origen de información de la cuenta o del grupo.

Acceder

En esta pestaña se ofrece una descripción general de a qué recursos o sistemas puede acceder esta identidad.



Asset Name	AES	Asset Class	Entitlements	Entitlement Provider	Trustees
dcadmin	917	Account	ACCESS_ALLOWED//ADS_RIGHT_DS_DELETE_CHILD//		4
dcadmin	917	Account	ACCESS_ALLOWED//WRITE_OWNER//		4
dcadmin	917	Account	ACCESS_ALLOWED//DELETE//		4

El mosaico incluye la siguiente información:

- **Nombre del activo:** enumera los nombres de los activos o cuentas administrados (por ejemplo, "dcadmin") asociados a la identidad.
- **AES:** Asset Exposure Score. Tenable calcula un AES dinámico para cada activo de la red para representar la exposición relativa del activo como número entero entre el 0 y el 1000. Un valor de AES más alto indica una mayor exposición. Tiene un valor numérico, aquí aparece 917 con un gráfico de barras que representa una medida relativa de seguridad o acceso. Para obtener más información, consulte [Tenable Inventory Metrics](#) (Métricas de Tenable Inventory).
- **Clase de activo:** indica el tipo de activo, que en este caso está etiquetado como "Cuenta". Los activos enumerados son cuentas de usuario o de sistema.
- **Derechos:** describe los permisos o derechos otorgados al activo. Por ejemplo, derechos como ACCESS_ALLOWED//ADS_RIGHT_DS_DELETE_CHILD//, WRITE_OWNER// y DELETE// definen los permisos específicos asociados a cada activo.
- **Proveedor de derechos:** especifica el origen o el servicio que proporcionan estos derechos.
- **Administradores:** muestra la cantidad de administradores asociados al activo, que representan personas o grupos que tienen control sobre el activo o son responsables de él (se muestran como 4 administradores por cada fila).

Tarjeta de exposiciones

Una tarjeta de exposiciones representa los datos entrantes de las etiquetas y orígenes de datos configurados. Agrupa y normaliza los datos para brindar una visualización de la métrica Cyber Exposure Score (CES) y otras. Los usuarios pueden crear tarjetas personalizadas o usar las tarjetas proporcionadas por Tenable para obtener información y orientación sobre qué áreas necesitan mayor atención.



- Haga clic en cualquier tarjeta para ir directamente a Lumin Exposure View, donde los datos de la tarjeta seleccionada aparece de manera predeterminada.

Relaciones

En la sección **Relaciones** se muestra una lista de todos los activos con una relación conocida con la identidad actual cuyos detalles está viendo.

Relationship Type	Direction	Asset Name	Class	AES	Weaknesses	Last Updated	
Link a Person to all their Accounts	Source	Cecil Bagley	Account	902	6	September 10, 2024	See details >
Link a Person to all their Accounts	Target	Cecil Bagley	Account	902	6	September 10, 2024	See details >

El mosaico incluye la siguiente información:

- **Tipo de relación:** tipo de relación entre las dos identidades.
- **Dirección:** indica si la identidad relacionada es el origen o el destino de la relación.
- **Nombre del activo:** identificador del activo de la identidad relacionada.
- **Clase de activo:** indica el tipo de activo, que en este caso está etiquetado como "Cuenta".
- **AES:** Asset Exposure Score. Tenable calcula un AES dinámico para cada activo de la red para representar la exposición relativa del activo como número entero entre el 0 y el 1000. Para obtener más información, consulte [Tenable Inventory Metrics](#) (Métricas de Tenable Inventory).
- **Debilidades:** debilidades asociadas al activo.
- **Última actualización:** fecha en la que un escaneo identificó el activo por última vez.



Aspectos esenciales de Identidad 360

Identidad 360 ofrece herramientas sólidas para administrar y analizar los datos de identidad de su organización para permitirle tomar decisiones de seguridad informadas.

Buscar

Identidad 360 ofrece tres potentes opciones de búsqueda para ayudarlo a encontrar la información exacta que necesita:

- **Generador de consultas de búsqueda global**

- Permite búsquedas complejas y precisas mediante propiedades específicas y consultas relacionales.
- Ideal para usuarios avanzados y análisis detallados.
- Ejemplo: Busque todas las cuentas que sean miembros de las “identidades que tienen cuentas que pertenecen a un grupo específico” o “identidades con derechos de alto riesgo a las que se accedió en los últimos 30 días”.
- Beneficios: Le permite construir búsquedas precisas de varias capas para identificar exactamente los datos que necesita.

Para obtener información completa sobre cómo usar este generador de consultas, consulte [Global Search Quick Reference Guide](#) (Guía de referencia rápida de búsqueda global).

- **Búsqueda de procesamiento del lenguaje natural (PLN)**

- Escriba la solicitud con sus propias palabras.
- El sistema interpreta su intención de manera inteligente y la convierte en una consulta estructurada.
- Ejemplo: “Quiero ver todas las cuentas de usuario inactivas en el departamento de Marketing”.
- Beneficios: Es fácil de usar, no exige conocimientos de sintaxis de consultas y es ideal para búsquedas particulares rápidas.



- **Búsqueda simple**

- Búsqueda basada en texto rápida y sencilla para obtener resultados inmediatos.
- Ideal para encontrar identidades específicas o búsquedas simples.
- Ejemplo: Escribir un nombre, como "Juan Pérez" o el ID de un empleado.
- Beneficios: Instantánea, ideal para operaciones diarias y verificaciones rápidas.

Cada tipo de búsqueda atiende diferentes necesidades y escenarios de los usuarios, desde análisis de datos complejos hasta búsquedas rápidas de identidades. Puede elegir el método de búsqueda más apropiado según la tarea actual, su experiencia técnica y la complejidad de la información que busca.

Filtrar

Una función de filtro en **Identidad 360** le permite aplicar criterios específicos para acotar o ajustar los datos que aparecen.

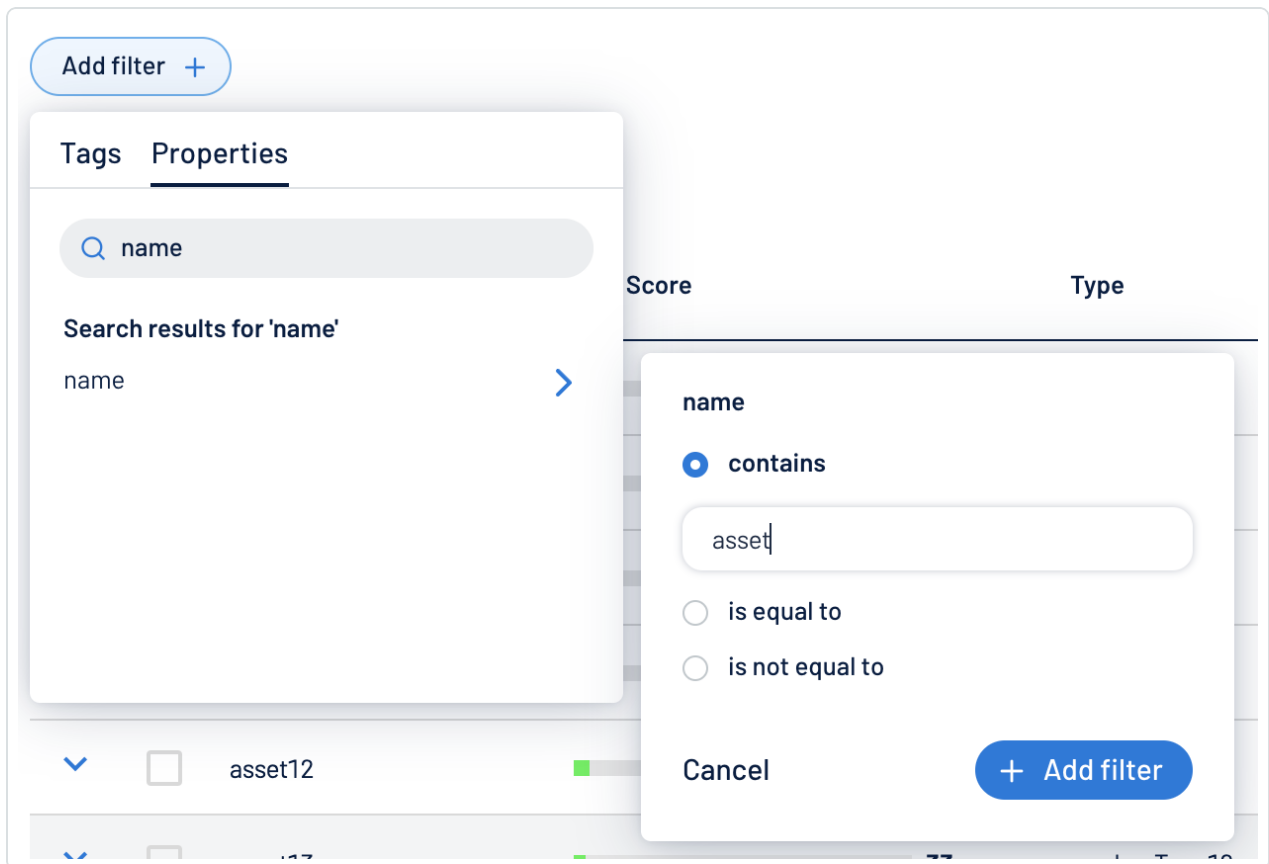
Para aplicar un filtro:

1. En el encabezado de la página "Identidades", haga clic en  .

Aparece el botón "Agregar filtro".

2. Haga clic en **Agregar filtro +**.

Aparece un menú.



3. Siga uno de los procedimientos a continuación:

- Para buscar la lista de activos por etiqueta, haga clic en **Etiquetas** (solo rige con la licencia de Tenable One y se gestiona en Tenable Inventory).
- Para buscar en la lista de activos por propiedad del activo, haga clic en **Propiedades**.

4. En el cuadro de búsqueda, escriba los criterios por los cuales quiere buscar en la lista de activos.

Tenable Inventory rellena una lista de opciones según los criterios.

5. Haga clic en la etiqueta o propiedad por la que quiere filtrar la lista de activos.

Aparece un menú.

6. Seleccione cómo aplicar el filtro. Por ejemplo, si quiere buscar un activo cuyo nombre es Asset14, seleccione el botón de selección "contiene" y, en el cuadro de texto, escriba "Asset14".

7. Haga clic en **Agregar filtro**.



El filtro aparece encima de la lista de activos.

8. Repita estos pasos para cada filtro adicional que quiera aplicar.
9. Haga clic en **Aplicar filtros**.


La página filtra la lista de identidades según los criterios designados.

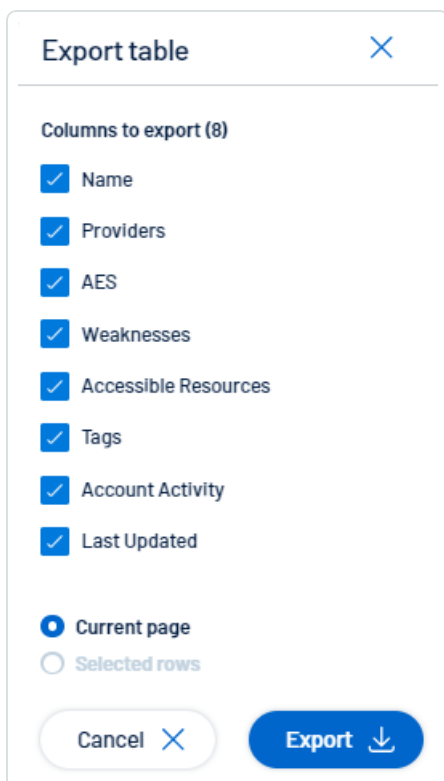
Exportar

Puede exportar los datos que aparecen en la tabla a un archivo Excel.

Nota: Cada pestaña dentro de la vista detallada "Identidad" ofrece su propia opción de exportación, lo que le permite extraer conjuntos de datos más específicos.

Para exportar datos:

1. En el encabezado de la página "Identidades", haga clic en el ícono .
2. En la ventana "Exportar tabla", seleccione las columnas que quiere exportar. Tiene la opción de exportar la página actual o las filas seleccionadas.




Export table ×

Columns to export (8)

- Name
- Providers
- AES
- Weaknesses
- Accessible Resources
- Tags
- Account Activity
- Last Updated

Current page
 Selected rows

Cancel × **Export** 




3. Haga clic en **Exportar**.

Personalizar columnas

















Puede agregar, quitar o reordenar columnas para adaptar la vista a sus preferencias. Si quiere revertir algún cambio, puede restablecer la configuración predeterminada en cualquier momento.


Para personalizar la visualización de las columnas:





1. En el encabezado de la página "Identidades", haga clic en .

Aparece la ventana "Personalizar columnas".

Customize columns ✕

Reorder added columns	Show / Hide	Remove
1.  Name <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
2.  Providers <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
3.  AES <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
4.  Weaknesses <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
5.  Accessible Resources <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
6.  Tags <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
7.  Account Activity <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
8.  Last Updated <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

 + Add columns

 Reset to defaults  ✕ Cancel   Apply columns

2. Opcional:

- En la sección **Reordenar las columnas agregadas**, haga clic en el nombre de una columna y arrástrelo para reordenar las columnas.



- En la sección **Mostrar/Ocultar**, seleccione las casillas o anule la selección para mostrar u ocultar las columnas en la tabla.
- En la sección **Quitar**, haga clic en el botón para quitar de manera permanente una columna de la tabla.
- Para agregar columnas a la tabla, haga clic en **Agregar columnas**.

Aparece la ventana **Agregar columnas a la tabla**.

- (Opcional) Utilice la barra de búsqueda para buscar una propiedad de una columna.
La lista de propiedades de columnas se actualiza según la consulta de búsqueda.
- Seleccione la casilla junto a las columnas que quiera agregar a la tabla.
- Haga clic en "Agregar".

La columna aparece en la ventana "Personalizar columnas".

3. Haga clic en **Aplicar columnas**.

El sistema guarda los cambios en las columnas de la tabla.

Columnas predeterminadas

El diseño predeterminado de las columnas garantiza que se pueda acceder fácilmente a los datos clave y, al mismo tiempo, ofrece flexibilidad para la personalización.

- **Nombre:** campo obligatorio que no se puede ocultar ni quitar, ya que sirve como identificador principal de cada elemento.
- **Proveedores:** muestra el servicio o la plataforma asociados que están vinculados al elemento.
- **AES:** muestra el Asset Exposure Score.
- **Debilidades:** resalta las vulnerabilidades o problemas detectados para los elementos enumerados.
- **Recursos accesibles:** muestra los recursos a los que puede acceder la cuenta o entidad.
- **Etiquetas:** etiquetas o metadatos asociados a cada elemento para ayudar con la categorización.



- **Actividad de la cuenta:** registros o métricas que están relacionados con la actividad de las cuentas.
- **Última actualización:** muestra la fecha más reciente en la que se actualizó el elemento.

Para restablecer las columnas predeterminadas:

- Haga clic en **Restablecer valores predeterminados** para restablecer todas las columnas a sus valores predeterminados.

Descripción de la pertenencia a inquilinos

La **pertenencia a inquilinos** representa un vínculo unidireccional entre dos tipos de activos en el ecosistema de un proveedor de identidad:

1. **Un activo del proveedor de identidad**, como una cuenta de usuario, un grupo o un recurso.
2. **El activo "inquilino"** representa la entidad o dominio más amplio que incluye al activo. La naturaleza del "inquilino" depende del proveedor de identidad específico.

Esta pertenencia a inquilinos ayuda a identificar relaciones entre los activos y sus inquilinos, lo que ofrece información sobre la organización y la jerarquía de los activos.

Vincular activos a un inquilino

Para Active Directory (AD), los activos se vinculan a su inquilino (dominio de AD) mediante el **nombre distintivo (DN)** del activo. El nombre distintivo proporciona información jerárquica sobre la ubicación del activo en la estructura del directorio, que se utiliza para determinar el inquilino.

Identificar al inquilino

Cuando un activo se corresponde con un objeto de AD (por ejemplo, un usuario o grupo), su inquilino se identifica de la siguiente manera:

- Extraiga el **nombre distintivo** del activo.
- Identifique al inquilino a partir de las entradas del **componente del dominio (DC)** del nombre distintivo.

Ejemplo



- Nombre distintivo del activo: CN=UserA,CN=Users,DC=tenable,DC=corp
- Inquilino: DC=tenable,DC=corp (representa al dominio de AD)

Casos especiales: descripción de los vínculos de los dominios raíz de bosques

En algunos casos, la relación entre un activo de Active Directory (AD) y su inquilino (dominio) puede no seguir la estructura esperada debido a la forma en que AD gestiona ciertos objetos. En esta sección se explican estos “casos especiales” con más detalle para mayor claridad.

Qué son los dominios raíz de bosques

Los bosques de Active Directory constan de uno o más dominios organizados jerárquicamente. El **dominio raíz del bosque** es el dominio superior de esta jerarquía e incluye a todos los demás dominios del bosque. Algunos objetos de AD hacen referencia al dominio raíz del bosque en sus nombres distintivos, incluso si pertenecen a un dominio diferente. Este comportamiento puede afectar la forma en que se identifican los inquilinos.

Cómo surgen los casos especiales

Al identificar a un inquilino a partir del nombre distintivo (DN) de un activo, los componentes del dominio (DC=...) normalmente indican el dominio del activo. Sin embargo, hay excepciones:

1. **Objetos de configuración de todo el bosque**

- Determinados objetos de AD están vinculados a configuraciones o ajustes que se aplican a todo el bosque en lugar de a un dominio específico.
- Estos objetos tienen nombres distintivos que terminan de la siguiente forma:
 - CN=Configuration,DC=...
- Estos objetos se vinculan al **dominio raíz del bosque** en lugar de a su dominio “real”.

Ejemplo

- Nombre distintivo: CN=Configuration,DC=forestRoot,DC=com
- Inquilino: **dominio raíz del bosque** (DC=forestRoot,DC=com)



2. Zonas DNS del bosque

- Algunos objetos gestionan las zonas DNS que se comparten en todo el bosque. Sus nombres distintivos terminan de la siguiente forma:
 - DC=ForestDnsZones,DC=...
- Estos objetos están asociados al **dominio raíz del bosque**, no a su dominio específico.

Ejemplo

- Nombre distintivo: DC=ForestDnsZones,DC=forestRoot,DC=com
- Inquilino: **dominio raíz del bosque** (DC=forestRoot,DC=com)

Por qué es importante

Comprender estos casos especiales es fundamental para interpretar con precisión la **pertenencia a inquilinos**. Entre las implicaciones clave se incluyen las siguientes:

1. La identificación del inquilino puede diferir de las expectativas

- Un objeto que parece pertenecer a un dominio específico puede estar vinculado al dominio raíz del bosque.
- Los objetos en los contextos de nomenclatura "**Configuration**" o "**ForestDnsZones**" se vinculan al **dominio raíz del bosque** debido a su alcance en todo el bosque.

2. Aclaraciones sobre jerarquía y alcance

- Los objetos vinculados al dominio raíz del bosque suelen tener una aplicabilidad más amplia, ya que gestionan o representan configuraciones en el nivel de bosque.

3. Uso en resolución de problemas y auditoría

- Las interpretaciones erróneas de estos casos podrían generar errores al auditar estructuras de dominios o solucionar problemas relacionados con las identidades.

Al comprender estos matices, podrá interpretar los hallazgos con seguridad y mantener la precisión en las tareas de auditoría y resolución de problemas.

Por qué eligió Tenable Identity Explorer "inquilino" como nombre del contenedor raíz



Se trata de un nombre genérico, no específico del IdP, para el contenedor raíz de cada proveedor de identidad (IdP) para garantizar que funcione en diferentes sistemas, como “inquilinos de Entra” y “dominios de AD”.

Se eligió el término “**inquilino**” porque es ampliamente comprendido en el ámbito de la gestión de identidades, es neutral en todas las plataformas y ya se ajusta a los estándares existentes, como Microsoft Entra. Esto garantiza claridad, coherencia y flexibilidad para gestionar diversas implementaciones del IdP.

Trail Flow

Trail Flow de Tenable Identity Exposure muestra la supervisión y el análisis en tiempo real de los eventos que afectan su infraestructura de AD. Le permite detectar vulnerabilidades críticas y las acciones de corrección recomendadas.

Con la página **Trail Flow**, puede retroceder en el tiempo y cargar eventos anteriores o buscar eventos específicos. También puede usar el cuadro de búsqueda situado al principio de la página para buscar amenazas y detectar patrones malintencionados.

Trail Flow hace un seguimiento de los siguientes eventos:

- **Cambios de usuarios y grupos:** incluye la creación, la eliminación y la modificación de cuentas y grupos.
- **Modificaciones de permisos:** incluye las modificaciones a los controles de acceso en objetos, como archivos, carpetas e impresoras.
- **Ajustes en la configuración del sistema:** involucra cambios en los objetos de política de grupo (GPO) y otras opciones críticas.
- **Actividades sospechosas:** incluye intentos no autorizados, escalamientos de privilegios y otros eventos que generan señales de alerta.

Tenable Identity Exposure ofrece estas funcionalidades para aprovechar los datos de Trail Flow:

- **Búsquedas y filtros:** es posible navegar de manera sencilla por el flujo de eventos mediante palabras clave o criterios específicos, lo que permite centrar la atención en las actividades pertinentes y minimizar el ruido externo.



- **Información detallada del evento:** cada entrada de evento ofrece detalles exhaustivos, que abarcan el objeto afectado, el usuario responsable del cambio, el protocolo utilizado y los indicadores de exposición (IoE) asociados.
- **Relaciones visualizadas:** refiere a la capacidad de ilustrar las relaciones entre los eventos, donde se destaca cómo actividades aparentemente no relacionadas pueden contribuir a una campaña de ataque más amplia.

Para acceder a Trail Flow:

- En Tenable Identity Exposure, haga clic en **Trail Flow** en la barra de navegación de la izquierda.

Se abre la página “Trail Flow” con una lista de eventos. Para obtener más información, consulte [Tabla “Trail Flow”](#).

ORIGEN	TIPO	OBJETO	RUTA	DOMINIO	FECHA (HHMMSS, YYYY-MM-DD)
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	16:19:28, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	16:08:00, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	15:49:29, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	15:27:20, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	15:19:29, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	15:07:01, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	14:49:28, 2024-11-13
LDAP	dnsNode	DC=HK-dct.CK=tk.yv4u.com.CN=MicrosoftDNS.DC=DomainDnsZones.DC=HK.DC=yv4u.DC		TK.YV4U	14:46:59, 2024-11-13
LDAP	qRLDistributionPoint	CN=TK.YV4U-CA.CN=TK-CS.CN=CDP.CN=Public Key Services.CN=Service.CN=ConfReq		TK.YV4U	14:38:00, 2024-11-13
LDAP	dnsNode	DC=HK-dct.CK=tk.yv4u.com.CN=MicrosoftDNS.DC=DomainDnsZones.DC=HK.DC=yv4u.DC		TK.YV4U	14:34:12, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	14:26:20, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	14:19:29, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	14:05:59, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	13:49:28, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	13:25:20, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	13:19:29, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	13:04:59, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	12:49:28, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	12:24:18, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	12:19:28, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	12:03:59, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	11:49:28, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	11:23:18, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	11:19:29, 2024-11-13
LDAP	dnsNode	DC=dc-vm.DC=tenable.ad.CN=MicrosoftDNS.DC=DomainDnsZones.DC=tenable.DC=rad		KHLAB	11:02:59, 2024-11-13

Para seleccionar un período de tiempo:

1. Al principio de la página **Trail Flow**, haga clic en el cuadro de calendario.
2. Seleccione una fecha inicial y una fecha final.
3. Haga clic en **Buscar**.

Tenable Identity Exposure actualiza la tabla “Trail Flow” con el período de tiempo seleccionado.



Para seleccionar un dominio:

1. Al principio de la página **Trail Flow**, haga clic en **n/n dominio >**.

Se abre el panel **Bosques y dominios**.

2. Seleccione los bosques y dominios.
3. Haga clic en **Filtrar selección**.

Tenable Identity Exposure actualiza la tabla "Trail Flow" con información del bosque y el dominio seleccionados.

Para ver un evento:

- En la tabla "Trail Flow", haga clic en una línea que contenga el evento que quiere explorar.

Aparece el panel "Detalles del evento". Para obtener más información, consulte [Detalles del evento](#).

Para pausar o reiniciar Trail Flow:

- Siga uno de los procedimientos a continuación:

- Haga clic en el ícono  para pausar Trail Flow.

Pausar Trail Flow detiene el desplazamiento vertical automático de los eventos más recientes mientras el análisis continúa ejecutándose en segundo plano y le permite ejecutar una búsqueda de eventos.

- Haga clic en el ícono  para reiniciar Trail Flow.

Para cargar los eventos siguientes o anteriores:

- En la página "Trail Flow", siga uno de los procedimientos a continuación:

- Haga clic en **Cargar eventos siguientes**.
- Haga clic en **Cargar eventos anteriores**.

Tabla "Trail Flow"



Tenable Identity Exposure enumera los eventos de la instancia de Active Directory en la tabla "Trail Flow" de forma continua a medida que se producen. Incluye la siguiente información:

Información	Descripción
Origen	<p>Indica el origen de cualquier cambio relacionado con la seguridad en las infraestructuras de AD.</p> <p>Hay dos orígenes posibles:</p> <ul style="list-style-type: none">• El protocolo ligero de acceso a directorios (LDAP) usado para comunicarse con la infraestructura de AD.• El protocolo de bloque de mensajes del servidor (SMB) usado para compartir archivos, impresoras, etc. <p>Tenable Identity Exposure analiza exhaustivamente el tráfico LDAP y SMB en la red para detectar anomalías y amenazas potenciales.</p> <div data-bbox="418 919 1479 1234" style="border: 1px solid blue; padding: 5px;"><p>Nota: Active Directory (AD) permite a los administradores crear políticas de grupo que controlan las opciones implementadas en las cuentas de usuarios y de máquina. El objeto de política de grupo (GPO) almacena estas opciones de control. La carpeta SYSVOL almacena archivos de GPO en el controlador de dominio. Es importante supervisar el contenido de los GPO para seguridad de la instancia de AD, ya que cada miembro del dominio puede aplicarlos o ejecutarlos con un alto nivel de privilegios.</p></div>
Tipo	<p>Muestra los elementos característicos de un evento, por ejemplo:</p> <ul style="list-style-type: none">• ACL modificada• SPN modificado• Miembro quitado• Nuevo miembro• Nueva confianza• Tipo de archivo desconocido agregado• Nuevo objeto• Objeto quitado



	<ul style="list-style-type: none">• Contraseña modificada• UAC modificado• Nuevo GPO vinculado• Vínculo de GPO quitado• Cambio de propietario• Cambio de nombre en un archivo• SPN creado• Error al restablecer la autenticación• Error de autenticación
Objeto	Indica la clase o extensión de archivo asociadas a un objeto de AD. Puede buscar un objeto de directorio (usuario, equipo, etc.) o un archivo con una extensión de nombre específica (ini, XML, csv).
Ruta	Indica la ruta completa a un objeto de AD para identificar la ubicación exclusiva de este objeto en la instancia de AD.
Directorio	Indica el directorio desde donde provino el cambio en la infraestructura de AD.
Fecha	Indica el momento del evento.


Buscar en Trail Flow con el asistente

El asistente de búsqueda le permite crear y combinar expresiones de consulta.

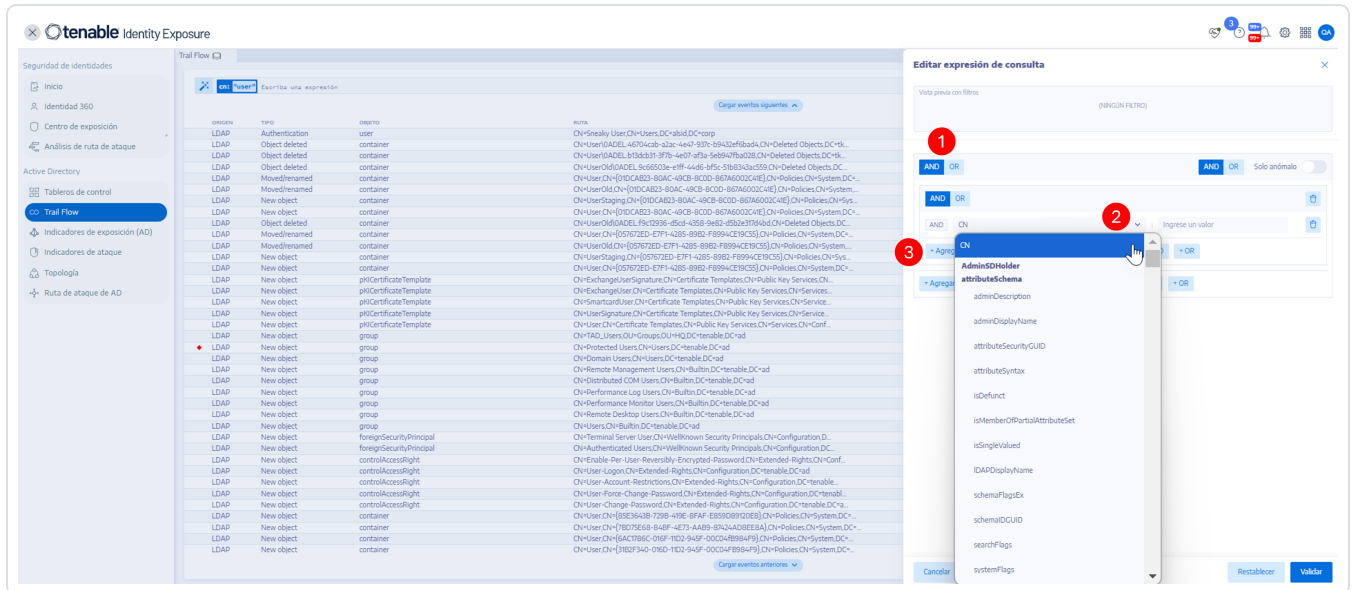
- Cuando se usan expresiones frecuentes en el cuadro de búsqueda, pueden agregarse a una lista de marcadores para usarlas más adelante.
- Cuando escribe una expresión en el cuadro de búsqueda, Tenable Identity Exposure guarda esta expresión en su panel "Historial" para que pueda reutilizarla.


Para buscar con el asistente:



1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página “Trail Flow”.
2. Haga clic en el ícono .

Se abre el panel **Editar expresión de consulta**. Para obtener más información, consulte [Personalizar las consultas de Trail Flow](#).



3. Para definir la expresión de consulta en el panel, haga clic en el botón del operador **AND** u **OR** (1) para aplicarlo en la primera condición.
4. Seleccione un atributo del menú desplegable e ingrese el valor (2).
5. Realice cualquiera de las acciones a continuación:
 - Para agregar un atributo, haga clic en **+ Agregar una nueva regla** (3).
 - Para agregar otra condición, haga clic en **Agregar una nueva condición** (operador **+AND** u **+OR**). Seleccione un atributo del menú desplegable e ingrese el valor.
 - Para restringir la búsqueda a objetos anómalos, haga clic en el conmutador **Solo anómalos** para establecerlo en “Permitir”. Seleccione el operador **+AND** u **+OR** para agregar la condición a la consulta.
 - Para eliminar una condición o regla, haga clic en el ícono .
6. Haga clic en **Validar** para ejecutar la búsqueda o en **Restablecer** para modificar las expresiones de consulta.



Consulte también

- [Buscar en Trail Flow de forma manual](#)
- [Buscar en Trail Flow con el asistente](#)
- [Personalizar las consultas de Trail Flow](#)
- [Marcar consultas](#)
- [Historial de consultas](#)

Buscar en Trail Flow de forma manual

Para filtrar eventos que coincidan con cadenas de caracteres o patrones específicos, puede escribir una expresión en el cuadro de búsqueda para ajustar los resultados mediante los operadores booleanos *, **AND** y **OR**. Puede encapsular instrucciones **OR** con paréntesis para modificar la prioridad de búsqueda. La búsqueda encuentra el valor específico en un atributo de Active Directory.

Para buscar en Trail Flow de forma manual:

1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página "Trail Flow".
2. En el cuadro de búsqueda, escriba una expresión de consulta.
3. Para filtrar los resultados de la búsqueda:
 - Haga clic en el cuadro **Calendario** para seleccionar una fecha inicial y una fecha final.
 - Haga clic en **n/n dominios** para seleccionar los bosques y dominios.
4. Haga clic en **Buscar**.

Tenable Identity Exposure actualiza la lista con los resultados que coinciden con los criterios de búsqueda.

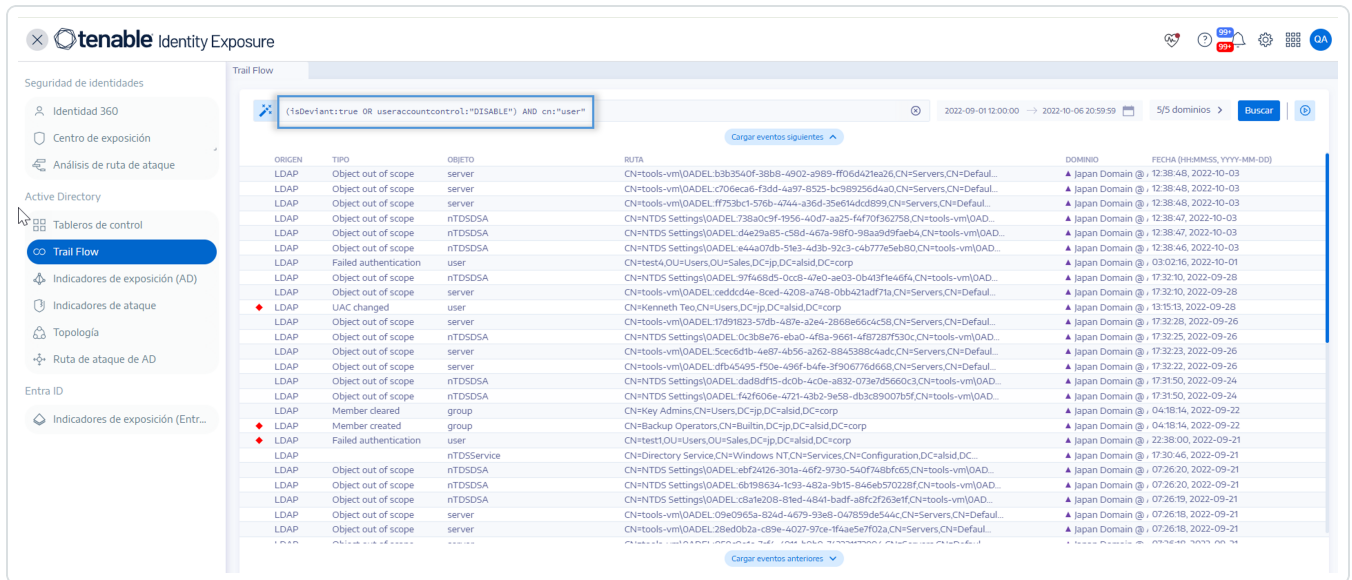
Consejo: Para buscar con otros criterios, puede [Buscar en Trail Flow con el asistente](#).

Ejemplo:

En el siguiente ejemplo se buscan:



- Cuentas de usuario desactivadas que puedan poner en peligro las infraestructuras de AD supervisadas.
- Actividades sospechosas y uso anómalo de cuentas.



Personalizar las consultas de Trail Flow

Trail Flow le permite ampliar las funcionalidades de Tenable Identity Exposure más allá de la supervisión predeterminada de indicadores de exposición e indicadores de ataque. Puede crear consultas personalizadas para recuperar datos rápidamente y, además, usar la consulta como alerta personalizada que Tenable Identity Exposure puede enviar a su sistema de administración de eventos e información de seguridad (SIEM).

En los siguientes ejemplos se muestran consultas personalizadas prácticas en Tenable Identity Exposure.

Caso de uso	Descripción
Binarios de arranque y apagado de GPO y supervisión de la ruta global de SYSVOL	<p>Supervisa los scripts en la ruta de arranque o la ruta de replicación global de SYSVOL. Los atacantes suelen usar estos scripts para aprovecharse de los servicios nativos de AD y propagar ransomware rápidamente por un entorno.</p> <ul style="list-style-type: none"> • Scripts en la consulta de la ruta de arranque:



globalpath: "sysvol" AND types: "Scriptsini"

Nota: Aquí, types hace referencia al atributo del objeto y no al encabezado de la columna.

- **Consulta de supervisión de SYSVOL:**

globalpath:"sysvol" AND (globalpath:".ps1" OR globalpath:".msi" OR globalpath:".bat" OR globalpath:".exe")

Modificaciones de la configuración de GPO

Supervisa las modificaciones en las configuraciones de un GPO. Los atacantes suelen usar este método para degradar la configuración de seguridad y así facilitar la persistencia o la toma de control de cuentas.

- **Consulta de supervisión de GPO:**

gptini-displayname:"New Group Policy Object" AND changetype:"Changed"

Error de autenticación y

Supervisa varios intentos fallidos de autenticación que



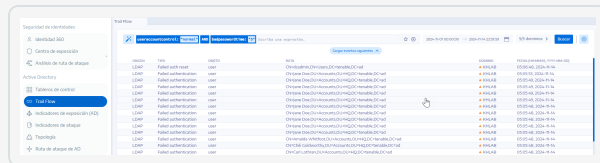
restablecimiento de contraseña

provocan un bloqueo, lo que puede servir como señal de alerta temprana de intentos de ataque de fuerza bruta.

Nota: Debe establecer la política de bloqueo y las variables de fecha/hora. Para obtener más información, consulte [Autenticación mediante una cuenta de Tenable Identity Exposure](#).

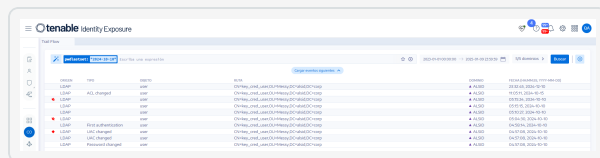
- **Consulta de error de autenticación:**

```
useraccountcontrol:"Normal" AND  
badpwdcount:"<ACCOUNT_LOCKOUT_  
THRESHOLD>" AND badpasswordtime:"<DATE_  
TIME_STAMP>"
```



- **Consulta de restablecimiento de contraseña:**

```
pwdlastset:"<DATE_TIME_STAMP"
```



Permisos de objeto agregados, quitados o modificados

Supervisa las modificaciones no autorizadas de los derechos de las ACL y los conjuntos de permisos de objetos relacionados. Los atacantes se aprovechan de este método para elevar los permisos.

Nota: Debe proporcionar la variable de fecha/hora.

- **Consulta de permisos de objeto:**



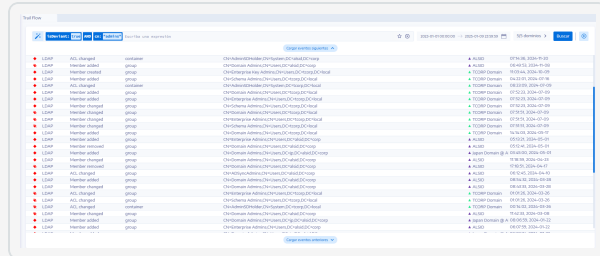
ntsecuritydescriptor:0 AND
wheneverchanged:"DATE_TIME_STAMP"



Cambios en los administradores, que provocan una anomalía

Los grupos administrativos integrados y los grupos personalizados son grupos confidenciales que requieren una supervisión minuciosa para detectar anomalías o cambios de configuración que puedan generar riesgos. Esta consulta le permite revisar rápidamente los cambios recientes que podrían haber afectado negativamente la configuración de seguridad dentro del grupo de administradores.

- **Consulta de cambios en administradores:**
`isDeviant:true AND cn:"admins"`



Consulte también


- [Buscar en Trail Flow de forma manual](#)
- [Buscar en Trail Flow con el asistente](#)
- [Marcar consultas](#)
- [Historial de consultas](#)
- [Casos de uso de Trail Flow](#)

Marcar consultas




Cuando se usan expresiones de consulta frecuentes, pueden agregarse a una lista de marcadores personalizados para usarlas nuevamente.

Para marcar una expresión de consulta:

1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página “Trail Flow”.
2. Haga clic en el ícono  junto al cuadro de búsqueda.

Se abre el panel **Editar expresión de consulta**.

3. En el cuadro de búsqueda, escriba una expresión de consulta.

4. Haga clic en el ícono  a la derecha del cuadro de búsqueda.

Aparece el cuadro **Agregar a los marcadores**.

5. En el cuadro **Elegir una carpeta**, haga clic en la flecha desplegable para seleccionar una carpeta de la lista.
6. (Opcional) Haga clic en el conmutador **Crear una carpeta nueva** para establecerlo en **Sí**. En el cuadro **Nombre de la carpeta**, escriba un nombre para la carpeta de marcadores.
7. En el cuadro **Nombre del marcador**, escriba un nombre para el marcador.
8. Haga clic en **Agregar**.

Un mensaje confirma que Tenable Identity Exposure agregó el marcador a la lista.

Para usar una expresión de consulta que se agregó a los marcadores:

1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página “Trail Flow”.
2. Haga clic dentro del cuadro de búsqueda.

Las pestañas **Historial** y **Marcadores** aparecen debajo del cuadro de búsqueda.

3. Haga clic en la pestaña **Marcadores**.

Aparece la lista de marcadores.

4. Haga clic en el marcador para seleccionarlo.

Tenable Identity Exposure carga la expresión de consulta y ejecuta la búsqueda.



Para gestionar los marcadores:

1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página "Trail Flow".

2. Haga clic dentro del cuadro de búsqueda.

Las pestañas **Historial** y **Marcadores** aparecen debajo del cuadro de búsqueda.

3. Haga clic en la pestaña **Marcadores**.

Aparece la lista de marcadores.

4. Haga clic en **Gestionar los marcadores**.

Se abre el panel **Marcadores**.

5. Realice cualquiera de las acciones a continuación:

◦ Buscar un marcador:

a. Escriba el nombre del marcador en el cuadro de búsqueda.

b. Seleccione una carpeta de la lista desplegable.

◦ Editar el nombre de un marcador o de una carpeta de marcadores:

a. Haga clic en el ícono  para el marcador o la carpeta de marcadores.

b. En el cuadro **Nombre del marcador** o **Nombre de la carpeta**, escriba un nombre nuevo para el marcador o la carpeta de marcadores.

c. Haga clic en **Editar**.

Un mensaje confirma que Tenable Identity Exposure actualizó el nombre del marcador o de la carpeta de marcadores.

◦ Eliminar un marcador de la carpeta de marcadores:

▪ Haga clic en el ícono  para el marcador o la carpeta de marcadores.

Consulte también

- [Buscar en Trail Flow de forma manual](#)
- [Buscar en Trail Flow con el asistente](#)



- [Personalizar las consultas de Trail Flow](#)
- [Historial de consultas](#)
- [Casos de uso de Trail Flow](#)

Historial de consultas

Cuando escribe una expresión en el cuadro de búsqueda, Tenable Identity Exposure guarda esta expresión en su panel **Historial** para que pueda reutilizarla.

Para utilizar una expresión de consulta en el historial:

1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página "Trail Flow".
2. Haga clic dentro del cuadro de búsqueda.

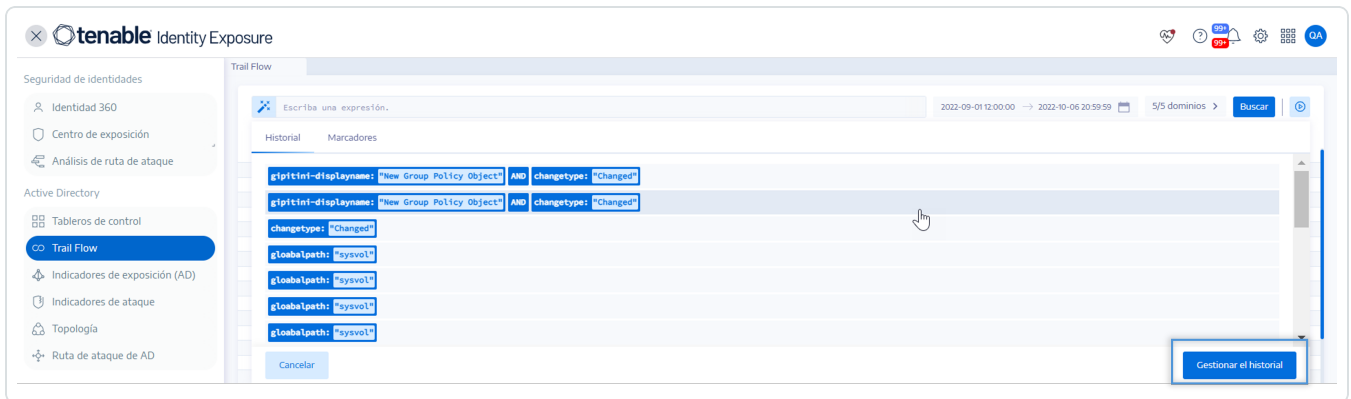
Las pestañas **Historial** y **Marcadores** aparecen debajo del cuadro de búsqueda.

3. Haga clic en la pestaña **Historial**.

Aparece la lista de expresiones de consulta.

4. Haga clic para seleccionar una expresión de consulta para usar.

Tenable Identity Exposure carga la expresión de consulta y ejecuta la búsqueda.



Para gestionar el historial de expresiones de consulta:

1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página "Trail Flow".
2. Haga clic dentro del cuadro de búsqueda.



Las pestañas **Historial** y **Marcadores** aparecen debajo del cuadro de búsqueda.


3. Haga clic en la pestaña **Historial**.

Aparece la lista de expresiones de consulta.

4. Haga clic en **Gestionar el historial**.

Se abre el panel **Historial**.

5. Realice cualquiera de las acciones a continuación:

- Buscar una expresión de consulta:
 - a. En el cuadro de búsqueda, escriba una expresión de consulta.
 - b. Haga clic en el cuadro del calendario para seleccionar una fecha inicial y una fecha final.
 - c. Haga clic en **Buscar**.
- Para eliminar una expresión de consulta del historial:
 - Haga clic en el ícono .
- Para borrar todas las expresiones de consulta del historial:
 - a. Haga clic en **Borrar selección**.

Aparece un mensaje para pedirle que confirme las eliminaciones.
 - b. Haga clic en **Confirmar**.

Consulte también


- [Buscar en Trail Flow de forma manual](#)
- [Buscar en Trail Flow con el asistente](#)
- [Personalizar las consultas de Trail Flow](#)
- [Marcar consultas](#)
- [Casos de uso de Trail Flow](#)

Mostrar eventos anómalos

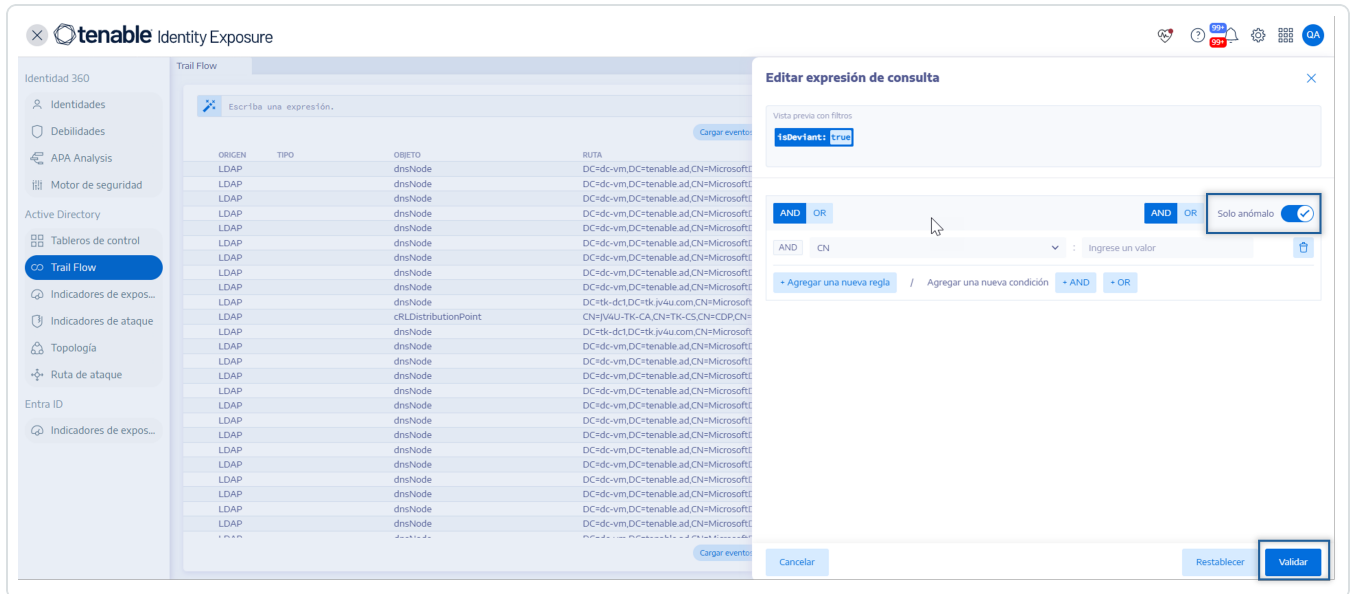


Puede concentrarse directamente en los eventos anómalos en la tabla "Trail Flow".

Para mostrar solo los eventos anómalos:

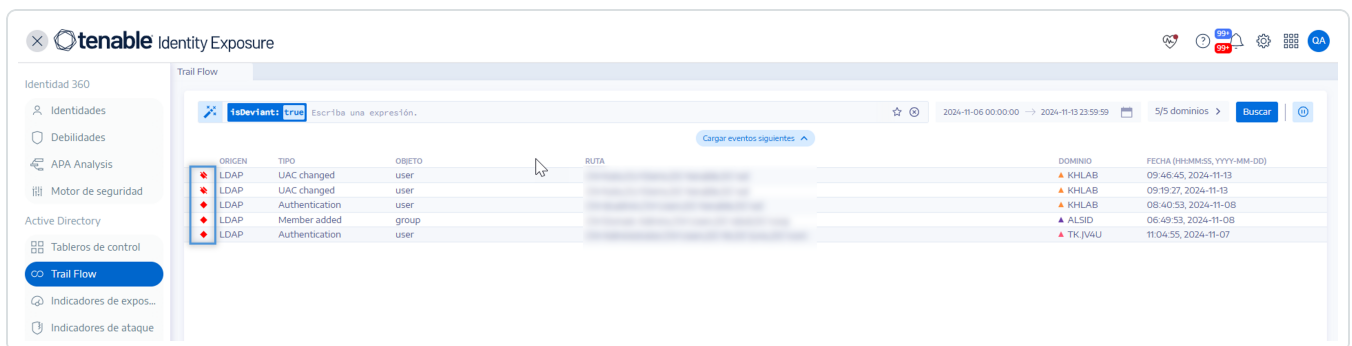
1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página "Trail Flow".
2. Haga clic en el ícono  junto al cuadro de búsqueda.

Se abre el panel **Editar expresión de consulta**.






3. Haga clic en el conmutador **Solo anómalo** para establecerlo en "Permitir".
4. Haga clic en **Validar**.

Tenable Identity Exposure actualiza la tabla "Trail Flow" con una lista de eventos con un diamante rojo junto al origen.



donde:



-  Trail Flow detectó una anomalía en el perfil de seguridad de Tenable Identity Exposure.
-  Trail Flow detectó una anomalía en otros perfiles de seguridad.
-  Muestra que los cambios resolvieron la anomalía.

Detalles del evento

Trail Flow en Tenable Identity Exposure brinda información detallada sobre cada evento que afecta su instancia de Active Directory (AD). Los detalles sobre un evento específico le permiten revisar la información técnica y adoptar medidas correctivas según lo exija el nivel de gravedad del indicador de exposición (IoE).

Para ver los detalles de un evento:

1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página “Trail Flow”.
2. Haga clic para seleccionar una entrada en la tabla “Trail Flow”.

Se abre el panel **Detalles del evento**.

IoE, evento y objeto anómalo

- Un **indicador de exposición** (IoE) describe una amenaza que afecta la instancia de AD. Los IoE de Tenable Identity Exposure evalúan los niveles de seguridad después de recibir un evento en tiempo real. Los IoE pueden incluir varias vulnerabilidades técnicas. Estos IoE brindan información sobre las vulnerabilidades detectadas, los objetos anómalos asociados y las recomendaciones para tomar medidas correctivas.
- Un **evento** indica un cambio relacionado con la seguridad que puede tener lugar en una instancia de AD. Puede ser un cambio de contraseña, la creación de un usuario, la creación o modificación de un GPO, un nuevo derecho delegado, etc. Un evento puede cambiar el estado de conformidad de un IoE y hacer que pase de estar en conformidad a no estarlo.
- Un **objeto anómalo** es un elemento técnico —ya sea por sí solo o asociado a otro objeto anómalo— que permite que el vector de ataque del IoE funcione. Para obtener más información, consulte [Indicadores de exposición](#).

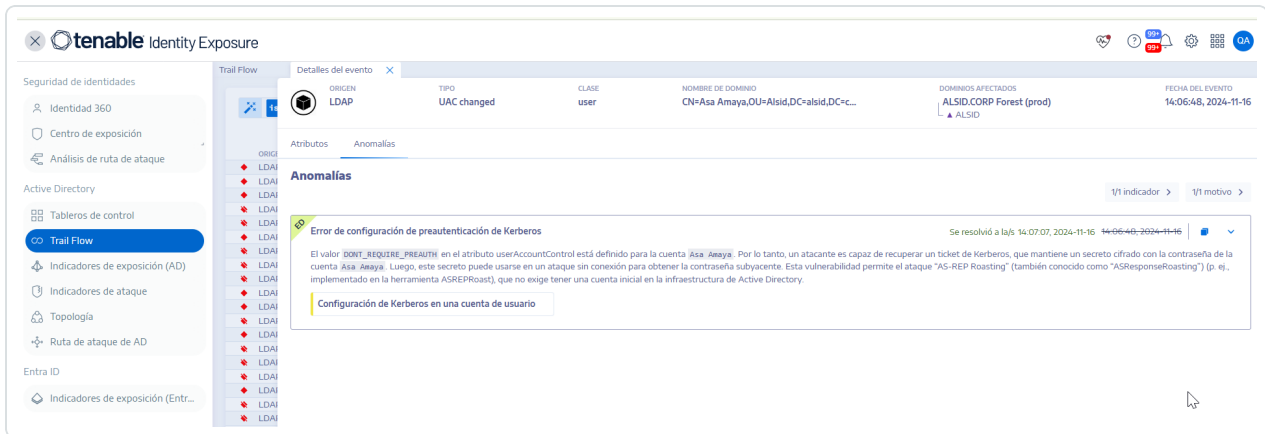


Tabla “Atributos”

La tabla “Atributos” incluye las siguientes columnas:

Columna	Descripción
Atributos	Indica los atributos del objeto de AD asociado al evento que seleccionó en la tabla “Trail Flow”. Los atributos describen las características del objeto. Varios atributos pueden describir un único objeto de AD.
Valor en el evento	Indica el valor del atributo en el momento en que ocurrió el evento.
Valor actual	Indica el valor del atributo en la instancia de AD en el momento en que lo está viendo.

Sugerencia: Para mostrar el valor del atributo antes de que ocurriera el evento, pase el cursor por el punto azul de la izquierda (si lo hay).

Para buscar un atributo:

- En el panel **Detalles del evento**, escriba una cadena en el cuadro de búsqueda.
Tenable Identity Exposure acota la lista a los atributos que coinciden con la cadena de búsqueda.

Para obtener más información, consulte [Cambios de atributos](#).

Anomalías



Si un evento en Trail Flow contiene anomalías, el panel “Detalles del evento” también las muestra para permitirle llegar al origen del problema.

Tenable Identity Exposure vincula una anomalía a un objeto raíz y puede vincularlo a varios atributos incriminatorios. Cuando resuelve uno de estos atributos, Tenable Identity Exposure resuelve la anomalía en el objeto raíz. Luego crea una nueva anomalía para el objeto raíz y mantiene el mismo motivo, pero incluye solo los atributos no resueltos.

Por ejemplo, Tenable Identity Exposure vincula una anomalía al objeto **A** por un único motivo que se conecta a varios objetos relacionados (**B**, **C** y **D**). Cuando resuelve el atributo incriminatorio en el objeto **C**, Tenable Identity Exposure resuelve la anomalía en el objeto **A**. Luego crea una nueva anomalía para el objeto **A** y la vincula al mismo motivo, pero incluye solo los objetos **B** y **D**.

Durante este proceso, Tenable Identity Exposure puede generar un evento de Trail Flow que muestre varias anomalías como resueltas y reabiertas en la misma marca de tiempo.

Para mostrar las anomalías:

1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página “Trail Flow”.
2. Haga clic para seleccionar una entrada en la tabla “Trail Flow”.

Se abre el panel **Detalles del evento**.

3. Seleccione la pestaña **Anomalías**.

Tenable Identity Exposure muestra la lista de anomalías y los IoE que las desencadenaron.

The screenshot shows the Tenable Identity Exposure web interface. On the left is a navigation sidebar with options like 'Seguridad de identidades', 'Identidad 360', 'Centro de exposición', 'Análisis de ruta de ataque', 'Active Directory', 'Tableros de control', 'Trail Flow' (highlighted), 'Indicadores de exposición (AD)', 'Indicadores de ataque', and 'Topología'. The main area is titled 'Detalles del evento' and contains a table with columns: ORIGEN (LDAP), TIPO (domainDNS), CLASE (domainDNS), NOMBRE DE DOMINIO, DOMINIOS AFECTADOS (TCORP Domain), and FECHA DEL EVENTO (06:16:25, 2024-11-18). Below the table, the 'Anomalías' tab is active, showing a list of anomalies. One anomaly is expanded, titled 'Reutilización de contraseñas dentro del dominio', with a description: 'Varios usuarios comparten la misma contraseña, lo que representa un enorme riesgo de seguridad. Si los atacantes logran vulnerar una de estas cuentas, pueden explotar esta vulnerabilidad a través de un ataque de difusión de contraseña para obtener acceso no autorizado a 2 cuentas más. Las cuentas siguientes comparten la misma contraseña, cuyo hash empieza por "2E6F7": Jaci, Box, Quinn, Shaw'. A sub-tab 'Detección de debilidades en contraseñas' is also visible.

Para acceder a los detalles de un IoE:



1. En la pestaña **Anomalías**, haga clic en el mosaico del loE debajo del motivo de la anomalía.

Se abre el panel **Detalles del indicador** con una lista de objetos anómalos y la siguiente información:

- Nombre del loE
- La gravedad del loE (crítica, alta, media, baja)
- El estado del loE
- La marca de tiempo de la última detección

2. Haga clic en cualquiera de las siguientes pestañas:

- **Información:** incluye recursos internos y externos sobre el loE.
- **Detalles de la vulnerabilidad:** brinda explicaciones sobre la debilidad detectada en la instancia de AD.
- **Objetos anómalos:** incluye detalles técnicos y un cuadro de búsqueda para filtrar los objetos.
- **Recomendaciones:** incluye sugerencias sobre cómo resolver el problema.

Cambios de atributos

Cuando cambia el valor de un atributo, Trail Flow muestra un punto azul antes de la columna **Atributo**.

Para mostrar el cambio de atributo:

1. En Tenable Identity Exposure, haga clic en **Trail Flow** en la barra de navegación de la izquierda.

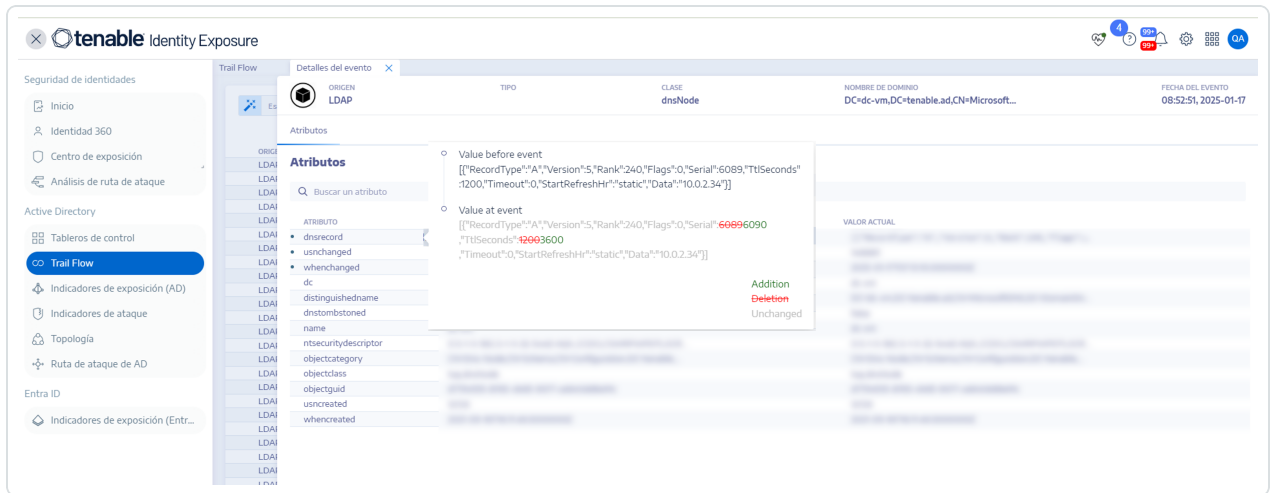
Se abre la página **Trail Flow** con una lista de eventos.

2. Pase el cursor por el punto azul delante de la línea de eventos para mostrar los cambios.

El color de la etiqueta **Valor en el evento** depende de los cambios que se apliquen al atributo:

- Verde: **adición**
- Rojo: **eliminación**

- Gris: **sin cambios**



Atributo "ntsecuritydescriptor"

Un descriptor de seguridad es una estructura de datos que contiene información de seguridad sobre un objeto de AD, como su titularidad y sus permisos. Para obtener más detalles, consulte la documentación de Microsoft en línea.

Para mostrar detalles del descriptor de seguridad de un objeto:

1. En Tenable Identity Exposure, haga clic en **Trail Flow** para abrir la página "Trail Flow".
2. Haga clic para seleccionar una entrada en la tabla "Trail Flow".

Se abre el panel **Detalles del evento**.



3. Pase el cursor por la entrada del atributo `ntsecuritydescriptor` (columna "Valor en el evento" o "Valor actual") **.

ORIGEN	TIPO	CLASE	NOMBRE DE DOMINIO	DOMINIOS AFECTADOS	FECHA DEL EVENTO
LDAP	UAC changed	user	CN=Kato,OU=Demo,DC=tenable,DC=ad	KHLAB forest KHLAB	09:46:45, 2024-11-13

ATRIBUTO	VALOR ACTUAL
useraccountcontrol	NORMAL
usnchanged	142702
whnchanged	2024-11-13T07:48:45.0000000Z
accountexpires	NEVER
badpasswordtime	1601-01-01T00:00:00.0000000Z
badpwdcount	0
cn	Kato
displayname	Kato
distinguishedname	CN=Kato,OU=Demo,DC=tenable,DC=ad
msds-supportedencryp...	
ntsecuritydescriptor	O:S-1-5-21-2331259844-3860294510-2117686686-512C:S-1-5-21-2331259844-3860294510-2117686686-512D A((OA,RP,4c164200-20c0-11d0-a768-00aa006e0529-5-1-5-21-2331259844-3860294510-2117686686-553)(OA,RP,5f202010-79a5-11d0-9020-00c04fc2d4cf-5-1-5-21-2331259844-3860294510-2117686686-553)(OA,RP,bc0ac240-79a9-11d0-9020-00c04fc2d4cf-5-1-5-21-2331259844-3860294510-2117686686-553)(OA,RP,037088f8-0ae1-11d2-b422-00a0-368f9399-5-1-5-21-2331259844-3860294510-2117686686-553)(OA,RP,WVP,bf9e7a7f-0de6-11d0-a285-...
objectcategory	CN=Person,CN=Schema,CN=Configuration,DC=tenable,DC=...
objectclass	top,person,organizationalPerson,user

4. Haga clic en **Ver descripción del SDDL**.

Se abre el panel **Descripción del SDDL**.

5. Haga clic en las flechas a la izquierda de "SDDL" (1), "DACL" (2) y "Descriptor" (3) para expandir la descripción:

Descripción del SDDL

1. SDDL
2. DACL
3. Descriptor
4. ACEs

Owner: Domain Admins
Group: Domain Admins
Flags: SE_DACL_AUTO_INHERITED

ACEs:

- > ACE
- > ACE
- > ACE
- > ACE
- > ACE

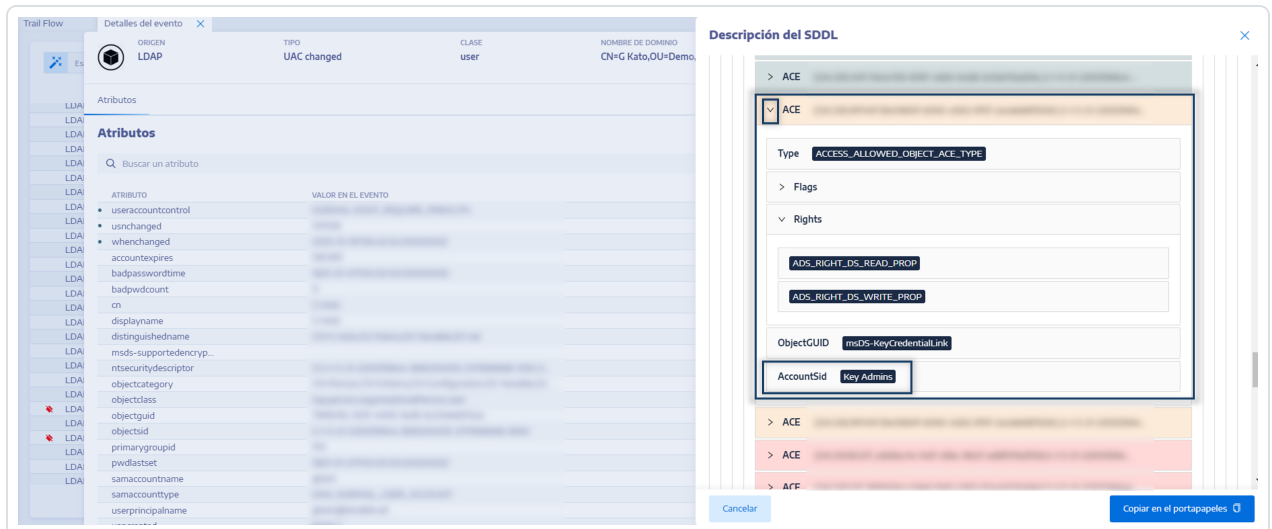
Cancelar Copiar en el portapapeles

6. Busque una entrada de control de acceso (ACE) (4) resaltada en color para mostrar los derechos de acceso del objeto. Los códigos de color indican:

- o **Rojo**: los usuarios tienen asignados derechos peligrosos y no deben tener derechos de acceso al objeto.



- **Naranja:** los usuarios privilegiados tienen asignados derechos peligrosos, pero en general tienen este tipo de derecho (por ejemplo: administradores de dominio).
- **Verde:** no hay derechos peligrosos.



7. Para copiar la descripción del SDDL, haga clic en **Copiar en el portapapeles**.

Casos de uso de Trail Flow

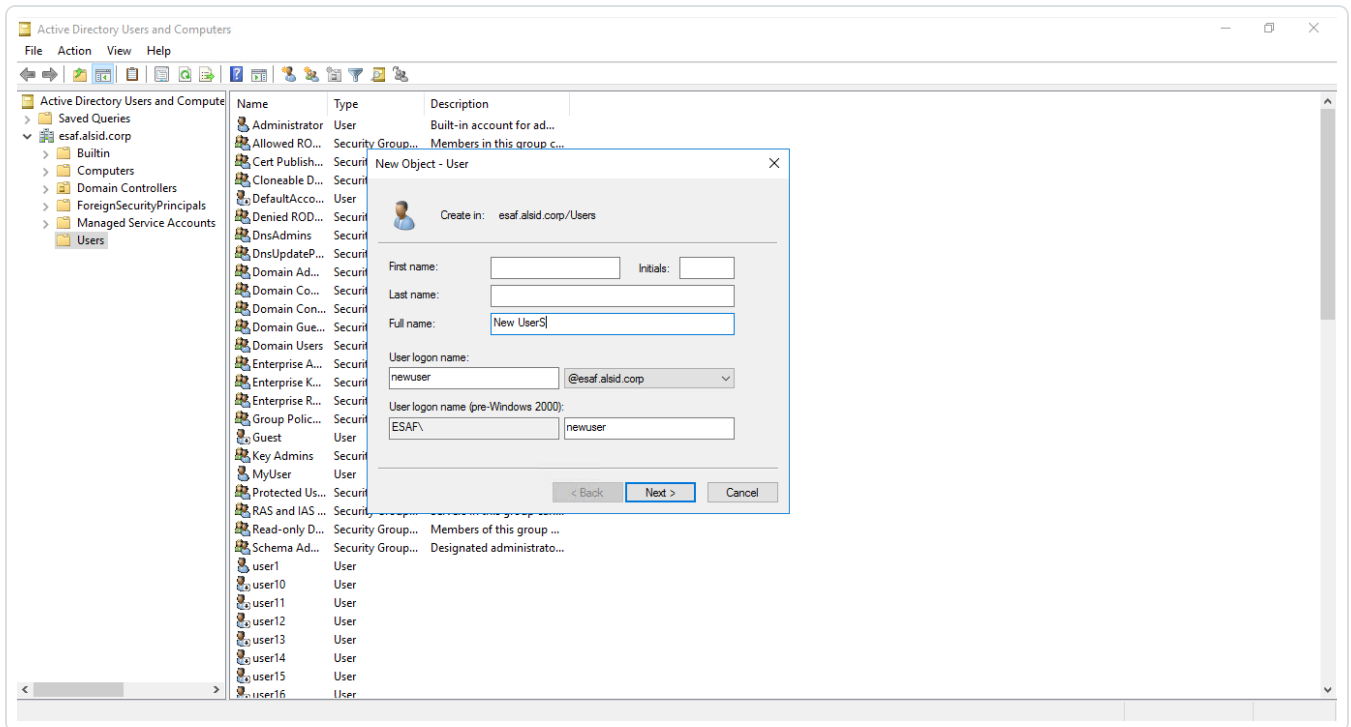
Para comprender el comportamiento de Trail Flow, dos ejemplos ilustran cómo una operación que lleva a cabo en la interfaz de Active Directory (AD) se ve reflejada en la página "Trail Flow".

Cada ejemplo compara los datos del lado del administrador (en la interfaz de AD) con los datos del lado del usuario final (en Tenable Identity Exposure). Independientemente de si se usa una aplicación, una API o un servicio para realizar una operación en la instancia de AD, el resultado en Trail Flow es el mismo.

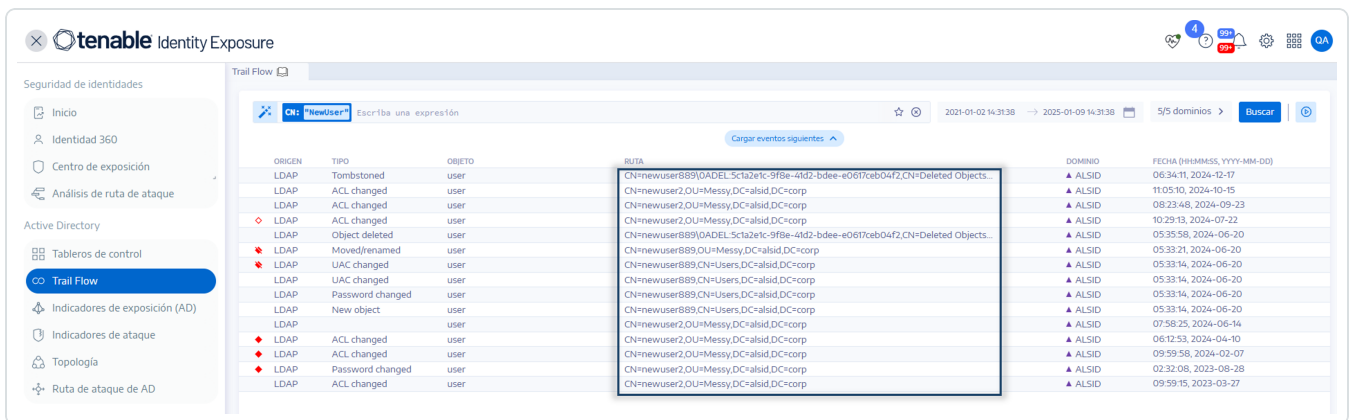
Nota: Estos ejemplos no son exhaustivos y no pueden cubrir todas las situaciones posibles.

¿Qué sucede en Trail Flow cuando se crea una nueva cuenta de usuario de AD?

- En el lado del administrador, usted ingresa diversa información sobre la nueva cuenta de usuario.



- En el lado del usuario final, Tenable Identity Exposure actualiza la página **Trail Flow**. Consulte la columna **Tipo**, que indica *Nuevo objeto*.



- En la página **Detalles del evento**, también se ve reflejado este cambio. Los puntos azules a la izquierda de los nombres de los atributos indican que se produjo una actualización.

Para obtener más detalles sobre los atributos, consulte [Ver los detalles de un evento](#).



Trail Flow

Detalles del evento

ORIGEN: LDAP

TIPO: Authentication

CLASE: user

NOMBRE DE DOMINIO: [dominio]

FECHA DEL EVENTO: 06:28:29, 2024-10-23

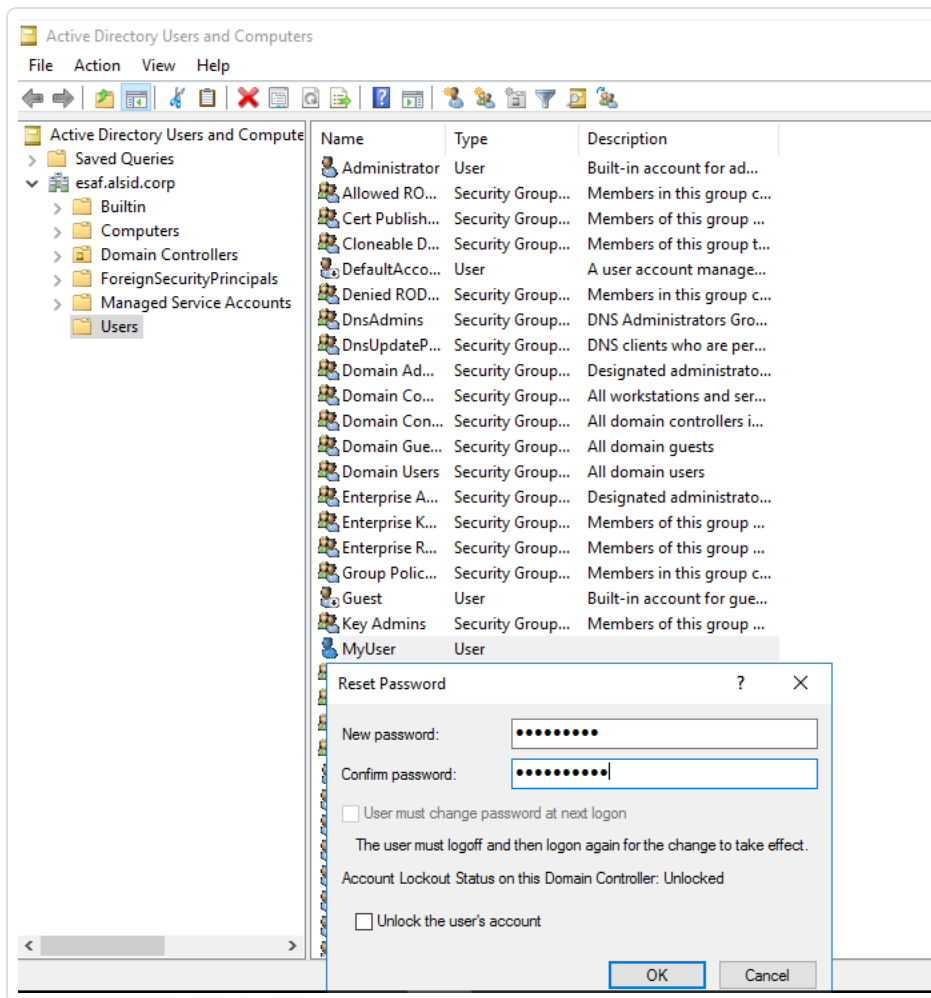
Atributos

Buscar un atributo

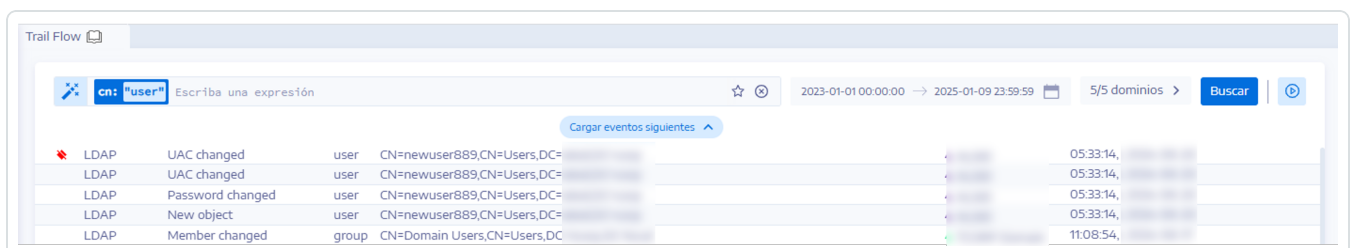
ATRIBUTO	VALOR EN EL EVENTO	VALOR ACTUAL
lastlogontimestamp	[valor]	[valor]
usnchanged	[valor]	[valor]
whentchanged	[valor]	[valor]
accountexpires	[valor]	[valor]
badpasswordtime	[valor]	[valor]
badpasswordcount	[valor]	[valor]
cn	[valor]	[valor]
displayname	[valor]	[valor]
distinguishedname	[valor]	[valor]
ms-ds-consistencygui...	[valor]	[valor]
ntsecuritydescriptor	[valor]	[valor]
objectcategory	[valor]	[valor]
objectclass	[valor]	[valor]
objectguid	[valor]	[valor]
objectsid	[valor]	[valor]
primarygroupid	[valor]	[valor]
pwdlastset	[valor]	[valor]
samaccountname	[valor]	[valor]
samaccounttype	[valor]	[valor]

¿Qué sucede en Trail Flow cuando se cambia la contraseña de un usuario de AD?

- En el lado del administrador, usted ingresa diversa información para restablecer la contraseña de un usuario.



- En el lado del usuario final, Tenable Identity Exposure actualiza la página **Trail Flow**. Consulte la columna **Tipo**, que indica “Contraseña modificada”.



- En la página **Detalles del evento**, también se ve reflejado este cambio con un punto azul a la izquierda del atributo whenchanged.



Para obtener más detalles sobre los atributos, consulte [Detalles del evento](#).

The screenshot shows the 'Detalles del evento' (Event Details) page in Trail Flow. The event type is 'Password changed' for user 'CN=user25,CN=...'. The interface includes a search bar for attributes and a table with the following data:

ATRIBUTO	VALOR EN EL EVENTO	VALOR ACTUAL
accountexpirytime	NEVER	NEVER
badpasswordtime	1601-01-01T00:00:00.0000000Z	2023-08-16T17:12:36.5985375Z
badpwdcount		
cn		
description		
displayname		
distinguishedname		
ntsecuritydescriptor		
objectcategory		
objectclass		
objectguid		
objectsid		
primarygroupid		
pwdlastset		
samaccountname		
samaccounttype		
telephonenumber		
useraccountcontrol		
userprincipalname		
whenchanged		
usncreated		
whencreated		

Consulte también

- [Buscar en Trail Flow de forma manual](#)
- [Buscar en Trail Flow con el asistente](#)
- [Personalizar las consultas de Trail Flow](#)
- [Marcar consultas](#)
- [Historial de consultas](#)

Indicadores de exposición

Tenable Identity Exposure usa indicadores de exposición (IoE) para medir la madurez de la seguridad de las infraestructuras de AD y asigna niveles de gravedad al flujo de eventos que supervisa y analiza. Tenable Identity Exposure desencadena alertas cuando detecta regresiones de seguridad.

Para mostrar los IoE:

1. En Tenable Identity Exposure, haga clic en **Indicadores de exposición** en el panel de navegación.



Se abre el panel **Indicadores de exposición**. De manera predeterminada, Tenable Identity Exposure muestra solo los loE que contienen anomalías.

2. (Opcional) Para mostrar todos los loE, haga clic en el conmutador **Mostrar todos los indicadores** para establecerlo en **Sí**.

Los loE de Tenable Identity Exposure vienen con una variedad de funcionalidades diseñadas para mejorar las capacidades de investigación:

- Búsqueda y filtros: aplique filtros basados en el bosque y el dominio para explorar los loE sin esfuerzo.
- Funcionalidad de exportación: el objeto anómalo le permitirá exportar los loE en formato CSV.
- Acción ante incidentes de loE: quite una exposición de la whitelist o vuelva a habilitarla.

Los datos del loE incluyen:

- Sección de información: en esta sección encontrará un resumen ejecutivo sobre cada indicador de exposición (loE), incluidas las herramientas de ataque conocidas, los dominios afectados y la documentación pertinente.
- Detalles de la vulnerabilidad: en esta sección se ofrece información más detallada sobre el error de configuración de Active Directory.
- Objetos anómalos: en esta sección se destacan los errores de configuración de Active Directory que pueden contribuir a superficies de ataque más amplias.
- Recomendación: esta sección lo guía por las estrategias de configuración efectivas para minimizar la superficie de ataque.

Para buscar un loE:

1. En la parte superior de la página **Indicadores de exposición**, escriba una cadena en el cuadro de búsqueda. Puede ser cualquier término relacionado con un loE, como contraseña, usuario, inicio de sesión, etc.
2. Presione Intro.

La página de loE se actualiza con los indicadores asociados al término de búsqueda.

Para filtrar los loE de un bosque o dominio en particular:



1. Haga clic en **n/n dominio**.

Se abre el panel **Bosques y dominios**.

2. Seleccione el bosque o el dominio.

3. Haga clic en **Filtrar selección**.

Nivel de gravedad

Los niveles de gravedad le permiten evaluar la gravedad de las vulnerabilidades detectadas y priorizar las acciones de corrección.

En el panel **Indicadores de exposición**, los loE se muestran de la siguiente manera:

- Por nivel de gravedad con códigos de colores.
- En dirección vertical: del más grave al menos grave (rojo para la prioridad máxima y azul para la prioridad mínima).
- En dirección horizontal: del más complejo al menos complejo. Tenable Identity Exposure calcula el indicador de complejidad de forma dinámica para indicar el nivel de dificultad para corregir el loE anómalo.

Gravedad	Descripción
Crítica: rojo	Muestra cómo prevenir los ataques y el riesgo de Active Directory por parte de ciertos usuarios sin privilegios.
Alta: naranja	Se ocupa de técnicas posteriores a la explotación que conducen al robo de credenciales o a la evasión de la seguridad, o de técnicas de explotación que requieren encadenamiento para ser peligrosas.
Media: amarillo	Indica un riesgo limitado para la infraestructura de Active Directory.
Baja: azul	Muestra prácticas recomendadas de seguridad. Ciertos contextos empresariales pueden permitir anomalías de bajo impacto que no necesariamente afecten la seguridad de AD. Estas anomalías tienen un impacto en la instancia de AD solo si un administrador comete un error, como activar una cuenta inactiva.

Fecha de detección y resolución de anomalías



A veces, Tenable Identity Exposure utiliza una fecha de detección o resolución diferente de la fecha real del evento. Esto sucede porque Tenable Identity Exposure almacena la fecha del evento más reciente que afecta a cada objeto de Active Directory (AD) durante el proceso de almacenamiento en caché.

Cuando Tenable Identity Exposure detecta y resuelve una anomalía que afecta a un objeto de AD, asigna la fecha del evento más reciente para ese objeto como fecha de resolución.

Por ejemplo, cuando cambia la pertenencia de un usuario a un grupo, Tenable Identity Exposure registra la fecha del evento para el grupo, no para el usuario. Si la anomalía que afecta al usuario se resuelve a través de un cambio de pertenencia al grupo, Tenable Identity Exposure usará la última fecha registrada del evento del usuario, no la fecha del cambio de pertenencia al grupo.

Consulte también

- [Detalles del indicador de exposición](#)
- [Objetos anómalos](#)
- [Buscar objetos anómalos](#)
- [Ignorar un objeto anómalo o un motivo \(anomalía\)](#)
- [Atributos incriminatorios](#)

Detalles del indicador de exposición

Los detalles de un indicador de exposición específico le permiten revisar la información técnica sobre las vulnerabilidades detectadas, los objetos anómalos asociados y las recomendaciones para la corrección.

Para mostrar los detalles del indicador de exposición:

1. En Tenable Identity Exposure, haga clic en **Indicadores de exposición** en el panel de navegación.

Se abre el panel **Indicadores de exposición**. De manera predeterminada, Tenable Identity Exposure muestra solo los IoE que contienen anomalías.



2. (Opcional) Para mostrar todos los loE, haga clic en el conmutador **Mostrar todos los indicadores** para establecerlo en **Sí**.
3. Haga clic en el mosaico de cualquier **indicador de exposición** en la página.

Se abre el panel **Detalles del indicador**.

En la parte superior, en el panel **Detalles del indicador** se resume la información ya proporcionada en la tabla "Trail Flow":

- El **Nombre** del loE.
- Su nivel de **Gravedad** (crítica, alta, media o baja).
- Su **Estado** de cumplimiento en función del resultado del último análisis que Tenable Identity Exposure ejecutó.
- La **Última detección**, que indica la última vez que Tenable Identity Exposure ejecutó el análisis.



4. Haga clic en cualquiera de las siguientes pestañas para obtener más detalles sobre el loE:

Pestaña	Descripción
Información	<p>Incluye recursos internos y externos sobre el loE, por ejemplo:</p> <ul style="list-style-type: none">• Resumen ejecutivo: una descripción general del problema para ayudarlo a tomar decisiones adecuadas.• Documentos: vínculos a recursos externos sobre el loE.• Herramientas conocidas por los atacantes: nombre de las herramientas de hackeo.• Una estructura de árbol de los dominios afectados.
Detalles de la vulnerabilidad	<p>Proporciona explicaciones sobre la debilidad detectada en la instancia de AD y los riesgos para Active Directory (AD) si no toma medidas correctivas.</p>
Objetos anómalos	<p>Los objetos anómalos revelan debilidades o comportamientos potencialmente peligrosos en la instancia de AD. Puede aplicar filtros a los objetos anómalos para identificar problemas críticos.</p> <p>Cuando el estado de un loE no está en conformidad e incluye objetos anómalos, puede tomar medidas de corrección para resolver las deficiencias de seguridad que Tenable Identity Exposure detectó. Para obtener más información, consulte Objetos anómalos.</p>
Recomendaciones	<p>Sugerencias sobre cómo restablecer el cumplimiento de sus requisitos de seguridad y mejorar la seguridad de su instancia de AD:</p> <ul style="list-style-type: none">• Un resumen ejecutivo ofrece una descripción general de la solución sugerida por Tenable Identity Exposure.• En la subsección "Detalles" se brindan consejos sobre cómo implementar el plan de acción y ayuda a los



	<p>administradores para iniciar los cambios necesarios en las infraestructuras de AD.</p> <ul style="list-style-type: none">• En la subsección “Documentos” se proporcionan vínculos a recursos externos sobre la solución sugerida o la amenaza.
--	---

Consulte también

- [Indicadores de exposición](#)
- [Objetos anómalos](#)
- [Buscar objetos anómalos](#)
- [Ignorar un objeto anómalo o un motivo \(anomalía\)](#)
- [Atributos incriminatorios](#)

Objetos anómalos

Los indicadores de exposición (IoE) de Tenable Identity Exposure pueden marcar objetos anómalos que revelan debilidades o comportamientos potencialmente peligrosos en una instancia de Active Directory (AD). Centrarse en estos objetos anómalos puede ayudarlo a detectar problemas críticos y corregirlos. Puede realizar cualquiera de las siguientes acciones:

- Buscar un objeto anómalo.
- Ignorar un objeto anómalo durante un período de tiempo.
- Seleccionar los bosques y dominios para buscar objetos anómalos.
- Obtener explicaciones sobre los atributos incriminatorios que afectan al IoE.
- Descargar un informe en el que se muestran todos los objetos anómalos.

Para mostrar los objetos anómalos:

1. En Tenable Identity Exposure, haga clic en **Indicadores de exposición** en el panel de navegación.



Se abre la página **Indicadores de exposición**. De manera predeterminada, Tenable Identity Exposure muestra solo los loE que contienen anomalías.

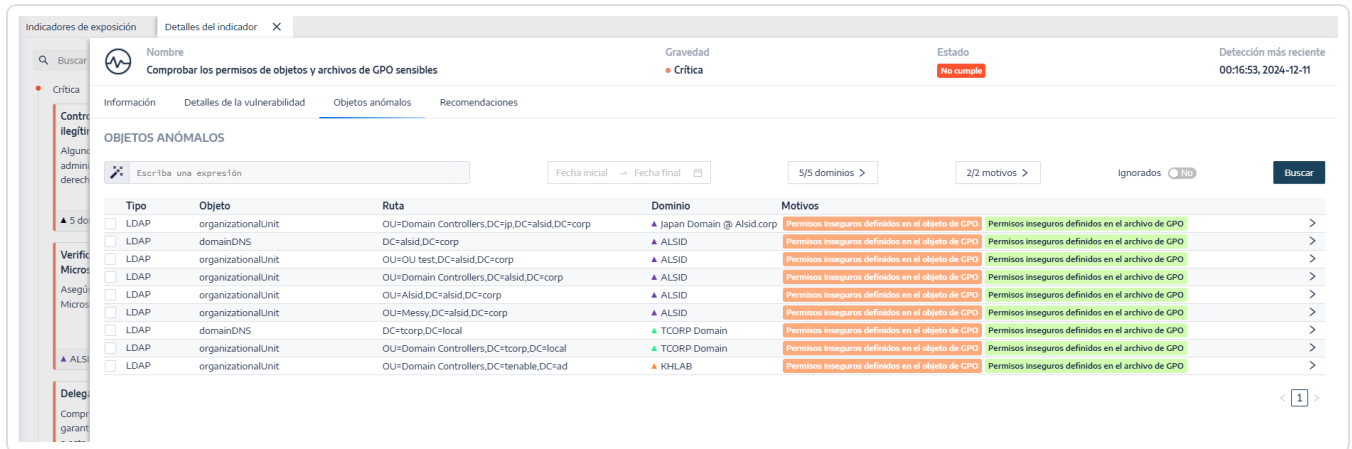
2. Haga clic en el mosaico de cualquier **indicador de exposición** en la página.

Se abre el panel **Detalles del indicador**.



3. Haga clic en la pestaña **Objetos anómalos**.

Aparece la lista de objetos anómalos asociados al loE.



La tabla de objetos anómalos incluye la siguiente información:

- **Tipo:** indica el origen de cualquier cambio relacionado con la seguridad en la instancia de AD (protocolos LDAP o SMB).
- **Objeto:** indica la clase o extensión de archivo asociadas a un objeto de AD.



- **Ruta:** indica la ruta completa a un objeto de AD para permitirle identificar la ubicación exclusiva en la instancia de AD.
- **Dominio:** indica el dominio de donde proviene el cambio en la instancia de AD.
- **Motivos:** enumera los atributos incriminatorios que afectan a los objetos anómalos.

Para exportar el informe de objetos anómalos:

1. Al final de la página **Objetos anómalos**, haga clic en **Exportar todo**.

Aparece el panel **Exportar objetos anómalos**.

2. En el cuadro **Formato de exportación**, haga clic en la flecha desplegable para seleccionar el formato.

3. Haga clic en **Exportar todo**.

Tenable Identity Exposure descarga en la máquina el informe de objetos anómalos.

Consulte también

- [Indicadores de exposición](#)
- [Detalles del indicador de exposición](#)
- [Buscar objetos anómalos](#)
- [Ignorar un objeto anómalo o un motivo \(anomalía\)](#)
- [Atributos incriminatorios](#)

Buscar objetos anómalos

Puede buscar objetos anómalos de forma manual o con el asistente.


Búsqueda con asistente

El asistente de búsqueda le permite crear expresiones de consulta.

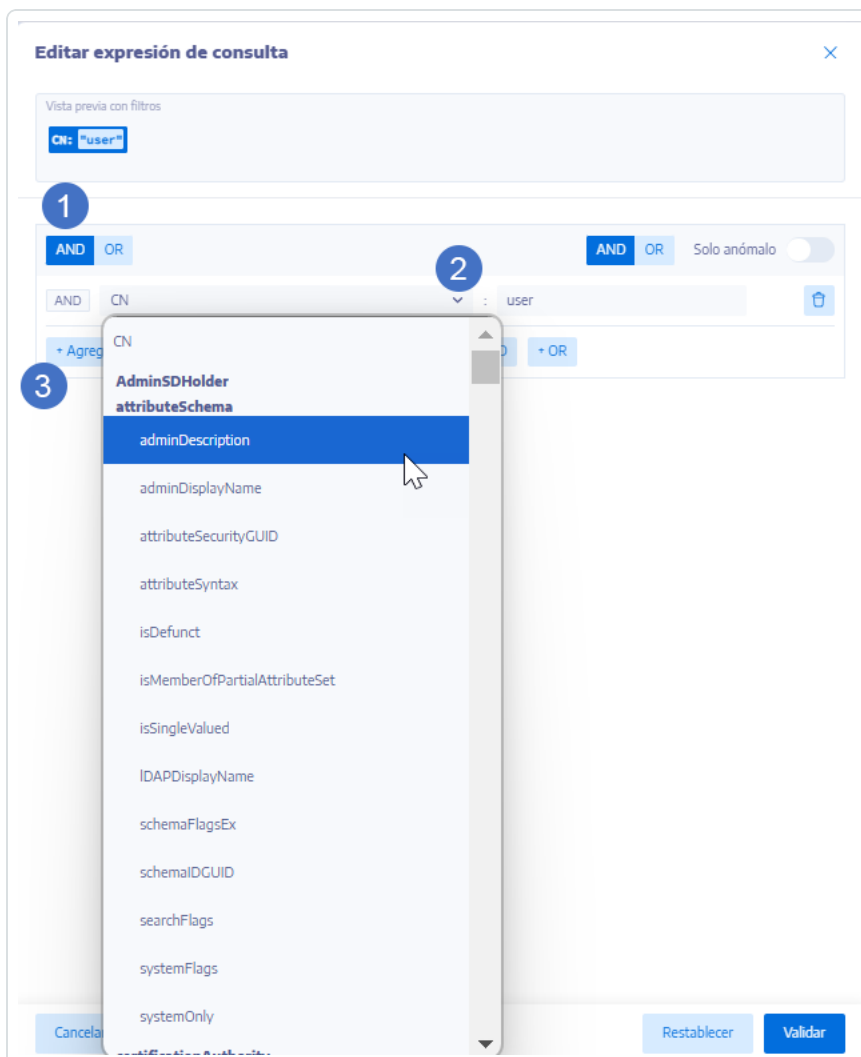


- Cuando se usan expresiones frecuentes en el cuadro de búsqueda, pueden agregarse a una lista de marcadores para usarlas más adelante.
- Cuando escribe una expresión en el cuadro de búsqueda, Tenable Identity Exposure guarda esta expresión en su panel "Historial" para que pueda reutilizarla.


Para buscar un objeto anómalo con el asistente:

1. Vaya a la lista de [Objetos anómalos](#).
2. Haga clic en el ícono .

Se abre el panel **Editar expresión de consulta**.





3. Para definir la expresión de consulta en el panel, haga clic en el botón del operador **AND** u **OR** (1) para aplicarlo en la primera condición.
4. Seleccione un atributo del menú desplegable e ingrese el valor (2).
5. Realice cualquiera de las acciones a continuación:
 - Para agregar un atributo, haga clic en **+ Agregar una nueva regla** (3).
 - Para agregar otra condición, haga clic en **Agregar una nueva condición** (operador **+AND** u **+OR**). Seleccione un atributo del menú desplegable e ingrese el valor.
 - Para restringir la búsqueda a objetos anómalos, haga clic en el conmutador **Solo anómalos** para establecerlo en "Permitir". Seleccione el operador **+AND** u **+OR** para agregar la condición a la consulta.
 - Para eliminar una condición o regla, haga clic en el ícono .
6. Haga clic en **Validar** para ejecutar la búsqueda o en **Restablecer** para modificar las expresiones de consulta.

Búsqueda manual

Para filtrar objetos anómalos que coincidan con cadenas de caracteres o patrones específicos, puede escribir una expresión en el cuadro de búsqueda para ajustar los resultados mediante los operadores booleanos *****, **AND** y **OR**. Puede encapsular instrucciones **OR** con paréntesis para modificar la prioridad de búsqueda. La búsqueda encuentra el valor específico en un atributo de Active Directory. Para buscar en Trail Flow de forma manual:

Para buscar un objeto anómalo de forma manual:



1. Vaya a la lista de [Objetos anómalos](#).

Tipo	Objeto	Ruta	Dominio	Motivos
LDAP	user	CN=svc.tenablead,CN=Managed Service Accounts,DC=tenable,DC=a...	KHLAB	Sin obligación de cambiar la contraseña
LDAP	user	CN=svc.tenablead,CN=Managed Service Accounts,DC=tk,DC=jv4u,D...	TKJV4U	Sin obligación de cambiar la contraseña

2. En el cuadro de búsqueda, escriba una expresión de consulta.

3. Para filtrar los resultados de la búsqueda:

- Haga clic en el cuadro **Calendario** para seleccionar una fecha inicial y una fecha final.
- Haga clic en **n/n dominios** para seleccionar los bosques y dominios.

4. Haga clic en **Buscar**.

Tenable Identity Exposure actualiza la lista con los resultados que coinciden con los criterios de búsqueda.

Gramática y sintaxis

Una expresión de consulta manual usa la siguiente gramática y sintaxis:

- Gramática: EXPRESIÓN [EXPRESIÓN DE OPERADOR]*
- Sintaxis: __CLAVE__ __SELECTOR__ __VALOR__

donde:

- __CLAVE__ hace referencia al atributo del objeto de AD que se va a buscar (como CN, userAccountControl, members, etc.)
- __SELECTOR__ hace referencia al operador: :, >, <, >= o <=.



- `__VALOR__` hace referencia al valor que se va a buscar.

Puede usar más claves para buscar contenido específico:

- `isDeviant` busca eventos que crearon una anomalía.

Puede combinar varias expresiones de consulta de Trail Flow con los operadores **AND** y **OR**.

Ejemplos:

- Busque todos los objetos que contengan la cadena `alicia` en el atributo de nombre común:
`cn:"alicia"`
- Busque todos los objetos que contengan la cadena `alicia` en el atributo de nombre común y que provocaron una anomalía específica: `isDeviant:"true" and cn:"alicia"`
- Busque un GPO denominado "Política de dominio predeterminada":
`objectClass:"groupPolicyContainer" and displayname:"Política de dominio predeterminada"`
- Busque todas las cuentas desactivadas con un identificador de seguridad que contenga S-1-5-21: `userAccountControl:"DISABLE" and objectSid:"S-1-5-21"`
- Busque todos los archivos `script.ini` en SYSVOL: `globalpath:"sysvol" and types:"SCRIPTSini"`

Nota: Aquí, `types` hace referencia al atributo del objeto y no al encabezado de la columna.

Consulte también

- [Indicadores de exposición](#)
- [Detalles del indicador de exposición](#)
- [Objetos anómalos](#)
- [Ignorar un objeto anómalo o un motivo \(anomalía\)](#)
- [Atributos incriminatorios](#)

Ignorar un objeto anómalo o un motivo (anomalía)



En Tenable Identity Exposure, un **objeto anómalo** hace referencia a cualquier objeto de la instancia de Active Directory (AD) que muestra comportamientos fuera de lo normal o de riesgo, como configuraciones o permisos inadecuados, que tienen el potencial de exponer vulnerabilidades de seguridad. Estos objetos se identifican a través de los indicadores de exposición (IoE) de Tenable, que detectan desviaciones con respecto a las prácticas recomendadas y las normas de seguridad.

Un **motivo**, también conocido como “**anomalía**”, es el atributo o factor específicos que hacen que un objeto sea anómalo. Existen varios motivos que pueden contribuir a que un IoE marque un objeto como anómalo. Por ejemplo, un objeto podría marcarse como anómalo debido a permisos de archivo incorrectos, errores de configuración o una delegación de riesgo, donde cada uno representa un “motivo” distinto.

En resumen:

- **Objeto anómalo:** objeto de AD marcado por su comportamiento fuera de lo normal o de riesgo.
- **Motivo/anomalía:** atributo o factor específicos que hacen que un IoE marque el objeto.

Estos motivos son fundamentales para comprender las debilidades de seguridad subyacentes asociadas a cada objeto anómalo.

Ignorar un objeto anómalo

Cuando se decide ignorar un objeto anómalo, también se ignoran todos los motivos o anomalías asociados.

Esto puede ser útil para poner orden en la interfaz cuando ciertos objetos marcados no son urgentes.

No obstante, ignorar estos objetos no resuelve los problemas subyacentes; simplemente evita que aparezcan en informes o pantallas de investigación durante el período de tiempo especificado.

Para ignorar objetos anómalos:

1. En Tenable Identity Exposure, vaya a la lista de [Objetos anómalos](#).
2. Seleccione las casillas junto a los objetos anómalos que quiere ignorar.
3. De manera opcional, puede filtrar los objetos anómalos para ignorarlos:



- Haga clic en el cuadro **Calendario** para seleccionar una fecha inicial y una fecha final.
- Haga clic en **n/n dominios** para seleccionar los bosques y dominios.

Sugerencia: Para una selección más rápida, puede marcar la casilla **Seleccionar todas las páginas** o **Seleccionar la página actual** al final de la página.

Tipo	Objeto	Ruta	Dominio	Motivos
<input type="checkbox"/>	LDAP	group	ALSID	Permisos inseguros en el grupo ADSyncAdmins
<input checked="" type="checkbox"/>	LDAP	msDS-GroupManagedServiceAccount...	ALSID	Permisos inseguros en el servicio de Microsoft Entra Connect
<input type="checkbox"/>	LDAP	user	ALSID	Permisos inseguros en el conector de AD DS
<input type="checkbox"/>	LDAP	user	ALSID	Permisos inseguros en el conector de AD DS
<input type="checkbox"/>	LDAP	user	ALSID	Permisos inseguros en el servicio de Microsoft Entra Connect

4. En la lista desplegable al final de la página, seleccione **Ignorar los objetos seleccionados**.

5. Haga clic en **Aceptar**.

Aparece el panel **Ignorar los objetos seleccionados**.

6. Haga clic en el cuadro **Ignorar hasta** para mostrar el calendario y seleccionar una fecha hasta la cual Tenable Identity Exposure debe ignorar el objeto anómalo.

7. Haga clic en **Aceptar**.

Tenable Identity Exposure muestra un mensaje de confirmación y actualiza la lista de objetos anómalos restantes.

Para mostrar los objetos anómalos que se ignoraron:

1. Haga clic en el conmutador **Ignorado** para establecerlo en **Sí**.
2. Al final de la página, haga clic en **Seleccionar todas las páginas**.
3. Seleccione **Dejar de ignorar los objetos seleccionados** de la lista desplegable.
4. Haga clic en **Aceptar**.



Aparece un panel de confirmación.

- Haga clic en **Aceptar** para validar los cambios.

Tenable Identity Exposure muestra los objetos anómalos ignorados.

Ignorar un motivo o "anomalía"

Cuando elige ignorar un motivo (o "anomalía") en particular en Tenable Identity Exposure, el IoE deja de enviar alertas sobre ese problema en concreto, pero no resuelve el problema en sí.

La anomalía ignorada ya no aparece en el tablero de control de supervisión activo, lo que, en definitiva, silencia la alerta por ese motivo específico.

Sin embargo, otras anomalías relacionadas con el mismo objeto continúan desencadenando alertas, a menos que también las ignore de forma individual.

Para ignorar un motivo ("anomalía"):

- En Tenable Identity Exposure, vaya a la lista de [Objetos anómalos](#).

Aparece una lista de objetos anómalos.

- Busque un objeto anómalo y haga clic en la flecha (>) al final de la línea.

La vista se expande para mostrar los detalles del motivo.

- Haga clic en la casilla al final de la línea. Si hay varios motivos, seleccione los que quiera ignorar o haga clic en **Seleccionar todo** para ignorar todos los motivos asociados.

The screenshot shows the Tenable Identity Exposure interface. At the top, there's a header with a logo, the title "Cuentas con privilegios que ejecutan servicios de Kerberos", a severity indicator "Gravedad" set to "Crítica", an "Estado" of "No cumple", and a "Detección más reciente" timestamp of "05:55:20, 2024-10-18". Below the header are tabs for "Información", "Detalles de la vulnerabilidad", "Objetos anómalos" (selected), and "Recomendaciones". The main content area displays a table of anomalous objects. The first row is expanded, showing details for a "Cuenta privilegiada con un SPN". The table has columns for "Tipo", "Objeto", "Ruta", "Dominio", and "Motivos". Below the table, there are checkboxes for "Anular selección de todo" and "1/1 objeto seleccionado", along with a dropdown menu for "Seleccionar una acción" and an "Aceptar" button. A context menu is open over the "Aceptar" button, showing options like "Ignorar las anomalías seleccionadas" and "Dejar de ignorar las anomalías seleccionadas".

- Haga clic en **Aceptar**.

Aparece el panel **Ignorar las anomalías seleccionadas**.




5. Haga clic en el cuadro **Ignorar hasta** para mostrar el calendario y seleccionar una fecha hasta la cual Tenable Identity Exposure debe ignorar la anomalía.
6. Haga clic en **Aceptar**.

Tenable Identity Exposure muestra un mensaje de confirmación y actualiza la lista de anomalías restantes.

Para mostrar las anomalías que se ignoraron:

1. Haga clic en el conmutador **Ignorado** para establecerlo en **Sí**.

La lista de objetos anómalos se actualiza con una vista ampliada de todos los motivos. Los motivos ignorados muestran el ícono .

2. Seleccione el motivo ignorado y haga clic en “Dejar de ignorar las anomalías seleccionadas” en la lista desplegable.

3. Haga clic en **Aceptar**.

Aparece el panel “Dejar de ignorar las anomalías seleccionadas”.

4. Haga clic en **Aceptar**.

Tenable Identity Exposure muestra un mensaje de confirmación y actualiza la lista de anomalías restantes.

Consulte también

- [Indicadores de exposición](#)
- [Detalles del indicador de exposición](#)
- [Objetos anómalos](#)
- [Buscar objetos anómalos](#)
- [Atributos incriminatorios](#)

Atributos incriminatorios



Tenable Identity Exposure muestra los atributos incriminatorios que desencadenan objetos anómalos en un indicador de exposición (IoE) y da los motivos para ayudarlo a comprender la anomalía y corregirla.

Para ver los atributos incriminatorios:

1. Vaya a la lista de [Objetos anómalos](#).

The screenshot shows the 'Objetos anómalos' section of the Tenable Identity Exposure interface. The indicator is 'Comprobar los permisos de objetos y archivos de GPO sensibles' with a severity of 'Crítica' and a status of 'No cumple'. The table lists 10 anomalous objects with columns for Tipo, Objeto, Ruta, Dominio, and Motivos. The 'Motivos' column contains two types of warnings: 'Permisos inseguros definidos en el objeto de GPO' and 'Permisos inseguros definidos en el archivo de GPO'.

Tipo	Objeto	Ruta	Dominio	Motivos
LDAP	organizationalUnit	OU=Domain Controllers,DC=jp,DC=alsid,DC=corp	Japan Domain @ Alsid.corp	Permisos inseguros definidos en el objeto de GPO
LDAP	domainDNS	DC=alsid,DC=corp	ALSID	Permisos inseguros definidos en el archivo de GPO
LDAP	organizationalUnit	OU=OU test,DC=alsid,DC=corp	ALSID	Permisos inseguros definidos en el objeto de GPO
LDAP	organizationalUnit	OU=Domain Controllers,DC=alsid,DC=corp	ALSID	Permisos inseguros definidos en el archivo de GPO
LDAP	organizationalUnit	OU=Alsid,DC=alsid,DC=corp	ALSID	Permisos inseguros definidos en el objeto de GPO
LDAP	organizationalUnit	OU=Messy,DC=alsid,DC=corp	ALSID	Permisos inseguros definidos en el archivo de GPO
LDAP	domainDNS	DC=corp,DC=local	TCORP Domain	Permisos inseguros definidos en el objeto de GPO
LDAP	organizationalUnit	OU=Domain Controllers,DC=tcorp,DC=local	TCORP Domain	Permisos inseguros definidos en el archivo de GPO
LDAP	organizationalUnit	OU=Domain Controllers,DC=tenable,DC=ad	KHLAB	Permisos inseguros definidos en el objeto de GPO

2. Haga clic en una entrada de la lista de objetos anómalos.

Tenable Identity Exposure muestra una lista de atributos incriminatorios para ese objeto anómalo:


The screenshot shows the details of an anomalous object. The object is 'organizationalUnit' with the path 'OU=Domain Controllers,DC=jp,DC=alsid,DC=corp' in the 'Japan Domain @ Alsid.corp' domain. The 'Motivos' column shows two warnings: 'PERMISOS INSEGUROS DEFINIDOS EN EL ARCHIVO DE GPO' and 'PERMISOS INSEGUROS DEFINIDOS EN EL OBJETO DE GPO'. The 'PERMISOS INSEGUROS DEFINIDOS EN EL ARCHIVO DE GPO' section lists dangerous entries in the GPO descriptor, including permissions for file write, append data, and write data. The 'PERMISOS INSEGUROS DEFINIDOS EN EL OBJETO DE GPO' section lists dangerous entries in the GPO object, including permissions for creating child objects.

La lista incluye la siguiente información:



- **Etiquetas codificadas por colores** para distinguir los diferentes motivos cuando haya varios.
- Valores:
 - ? : un valor de atributo faltante (vacío) que indica un comportamiento anormal.
 - No hay ninguna descripción disponible para esta anomalía: la detección se remonta a la versión 2.6, y Tenable Identity Exposure ya no gestiona este atributo.

Para copiar el atributo incriminatorio:

- Seleccione el atributo y haga clic en el ícono .

Consulte también

- [Indicadores de exposición](#)
- [Detalles del indicador de exposición](#)
- [Objetos anómalos](#)
- [Buscar objetos anómalos](#)
- [Ignorar un objeto anómalo o un motivo \(anomalía\)](#)

Indicadores de exposición basados en RSoP

Tenable Identity Exposure usa un conjunto de indicadores de exposición (IoE) basados en RSoP (conjunto resultante de políticas) para evaluar y garantizar la seguridad y el cumplimiento de varios aspectos. En esta sección se brinda información sobre el comportamiento actual de los IoE basados en RSoP específicos y cómo Tenable Identity Exposure aborda los problemas de rendimiento asociados con sus cálculos.

Los siguientes IoE dependientes de RSoP están involucrados en el marco de seguridad de Tenable Identity Exposure:

- Restricciones de inicio de sesión para usuarios privilegiados
- Privilegios sensibles peligrosos
- Aplicación de políticas de contraseñas débiles en los usuarios



- Endurecimiento insuficiente frente al ransomware
- Configuración sin protección del protocolo Netlogon

Estos loE dependen de una caché de resultados de cálculo de RSoP que se inicializa cuando es necesario y calculan valores que se agregan a pedido en lugar de depender de valores preexistentes. Anteriormente, los cambios en `AdObjects` desencadenaban la invalidación de la caché, lo que generaba un recálculo frecuente durante las ejecuciones de RSoP del loE.

Tenable Identity Exposure aborda el impacto en el rendimiento asociado a los cálculos de RSoP de la siguiente manera:

1. **Análisis de loE en vivo con datos potencialmente obsoletos:** el cálculo (evento de entrada/salida) de los loE que dependen del RSoP se lleva a cabo en tiempo real a medida que ocurren, incluso si los datos usados para el procesamiento no son los más actuales. Los eventos almacenados en búfer que tienen el potencial de invalidar la caché del RSoP permanecen almacenados hasta que cumplen una condición específica, lo que provoca el cálculo previsto.
2. **Invalidación de RSoP programado:** al cumplirse la condición para el recálculo, el sistema invalida la caché del RSoP, teniendo en cuenta los eventos almacenados en búfer durante el proceso de invalidación.
3. **Reejecución de los loE con caché actualizada:** luego de la invalidación de la caché, los loE se vuelven a ejecutar con la versión más reciente de `AdObject` de la caché, incorporando los eventos almacenados en búfer. Tenable Identity Exposure calcula cada loE individualmente para cada evento almacenado en búfer.

Por estos motivos, la duración de cálculo optimizada para los loE que dependen del RSoP provoca un cálculo más lento de las anomalías relacionadas con el RSoP.

Mejoras

Tenable Identity Exposure implementó cambios en los indicadores de exposición relacionados con las tareas del RSoP para mejorar el rendimiento general y la capacidad de respuesta.

- **Controles de seguridad más inteligentes:** un rediseño de cómo realizamos ciertos controles de seguridad (llamadas verificaciones de RSoP) para reducir las ralentizaciones del sistema.



- **Programación adaptable:** el sistema elegirá automáticamente los mejores momentos para ejecutar estas verificaciones en función de la carga de trabajo actual.
- **Protección contra sobrecarga:** hemos puesto en práctica nuevas medidas para evitar la sobrecarga del sistema durante períodos de mucha actividad.
- **Análisis de seguridad de archivos de GPO:** los indicadores de exposición que analizan la seguridad de los archivos de GPO ahora se procesarán cada 30 minutos y no en tiempo real, como sucede con otros loE.

Beneficios

- **Mejores tiempos de respuesta:** al optimizar el proceso de verificación de la seguridad, debería observar respuestas más rápidas del sistema, en especial durante las horas pico de uso.
- **Confiabilidad mejorada:** la nueva programación adaptable ayuda a garantizar que los controles de seguridad importantes no interfieran con su trabajo.
- **Experiencia más fluida:** con una mejor protección contra sobrecargas, el sistema debería mantener un rendimiento constante, incluso en caso de uso intensivo.
- **Estabilidad mejorada de la plataforma:** estos cambios beneficiarán en particular a los clientes con alta actividad de AD, lo que garantizará un rendimiento más uniforme.

Aspectos técnicos

- Las verificaciones de RSoP y los análisis de seguridad de archivos de GPO se ejecutan periódicamente y no en tiempo real.
- Cada 30 minutos, la plataforma evalúa su carga de trabajo. Si determina que puede hacer un análisis, procede; de lo contrario, espera hasta que la carga disminuya.
- Se implementó un algoritmo para detectar la sobrecarga del sistema, que tiene en cuenta factores como la longitud de la cola de mensajes y las tendencias de procesamiento.
- Durante los períodos de sobrecarga, las verificaciones no críticas se posponen para mantener la capacidad de respuesta del sistema.

Corregir las anomalías de los indicadores de exposición



Tenable Identity Exposure desencadena alertas cuando un indicador de exposición (IoE) encuentra objetos anómalos que requieren corrección.

Los siguientes son ejemplos en los que se muestra cómo llevar a cabo un procedimiento de corrección para tres IoE específicos.

- [Atributo adminCount definido en usuarios estándar](#)
- [Delegación peligrosa de Kerberos.](#)
- [Asegurar la coherencia de SDProp.](#)

Para obtener información completa sobre los IoE, consulte la documentación que se brinda en la interfaz de usuario de Tenable Identity Exposure.

Atributo adminCount definido en usuarios estándar

El atributo `adminCount` en una cuenta de usuario indica su pertenencia anterior en un grupo administrativo y no se restablece cuando la cuenta abandona el grupo. Como consecuencia, incluso las cuentas administrativas antiguas tienen este atributo, lo que bloquea la herencia de los permisos de Active Directory. Si bien originalmente se diseñó para proteger a los administradores, puede crear problemas difíciles con los permisos.

Este IoE de nivel medio solo informa sobre cuentas de usuarios y grupos activos con este atributo y excluye a los grupos privilegiados con miembros legítimos que tengan el atributo `adminCount` establecido en **1**.

Para corregir un objeto anómalo del IoE **Atributo adminCount definido en usuarios estándar**:

1. En Tenable Identity Exposure, haga clic en **Indicadores de exposición** en el panel de navegación para que se abra.

De manera predeterminada, Tenable Identity Exposure muestra solo los IoE que contienen objetos anómalos.

2. Haga clic en el mosaico del IoE **Atributo adminCount definido en usuarios estándar**.



Indicadores de exposición

- Media
- Cuentas inactivas: Detecta cuentas inactivas sin usar que pueden generar riesgos de seguridad. 5 dominios, Complejidad
- Integridad de Property Sets: Comprueba la integridad de property sets y valida los permisos. 5 dominios, Complejidad
- Endurecimiento insuficiente frente al ransomware: Se asegura de que el dominio haya implementado medidas de endurecimiento para protegerse frente al ransomware. 5 dominios, Complejidad
- Usuarios con permiso para unir equipos al dominio: Compruebe que los usuarios normales no puedan unir equipos externos al dominio. 5 dominios, Complejidad
- Uso reciente de la cuenta Administrador predeterminada: Comprueba los usos recientes de la cuenta de administrador integrada. 4 dominios, Complejidad
- Atributo AdminCount definido en usuarios estándar: Comprueba el atributo adminCount en cuentas dadas de baja, lo que lleva a problemas de permisos que son difíciles de administrar. 4 dominios, Complejidad
- Cuenta de usuario con contraseña antigua: Comprueba las actualizaciones periódicas de todas las contraseñas de cuentas activas en Active Directory para reducir el riesgo de robo de credenciales. 5 dominios, Complejidad
- Errores de configuración en cuentas de servicios: Muestra errores de configuración potenciales de las cuentas de servicios de dominio. 3 dominios, Complejidad
- Administración de cuentas administrativas locales: Garantiza la administración segura y centralizada de las cuentas administrativas locales mediante LAPS. 5 dominios, Complejidad
- Configuración de Kerberos en una cuenta de usuario: Detecta las cuentas que usan una configuración débil de Kerberos. 5 dominios, Complejidad
- Contraseñas reversibles: Comprueba que no pueda habilitarse la opción para almacenar contraseñas en un formato reversible. 5 dominios, Complejidad
- Contraseñas reversibles en GPO: Comprueba que las preferencias de los GPO no permitan contraseñas en un formato reversible. 2 dominios, Complejidad

Se abre el panel **Detalles del indicador**.

- Pase el cursor por el objeto anómalo y haga clic en él para mostrar los detalles y anote el nombre del dominio y la cuenta. (En este ejemplo: Dominio = OLYMPUS.CORP, y la cuenta estándar es unpriv-usr).

Indicadores de exposición Detalles del indicador X

Nombre: Atributo AdminCount definido en usuarios estándar Gravedad: Media Estado: No cumple Detección más reciente: 09:38:46, 2024-11-29

Información Detalles de la vulnerabilidad **Objetos anómalos** Recomendaciones

OBJETOS ANÓMALOS

Escriba una expresión Fecha inicial → Fecha final 5/5 dominios > 1/1 motivo > Ignorados 0/0 Buscar

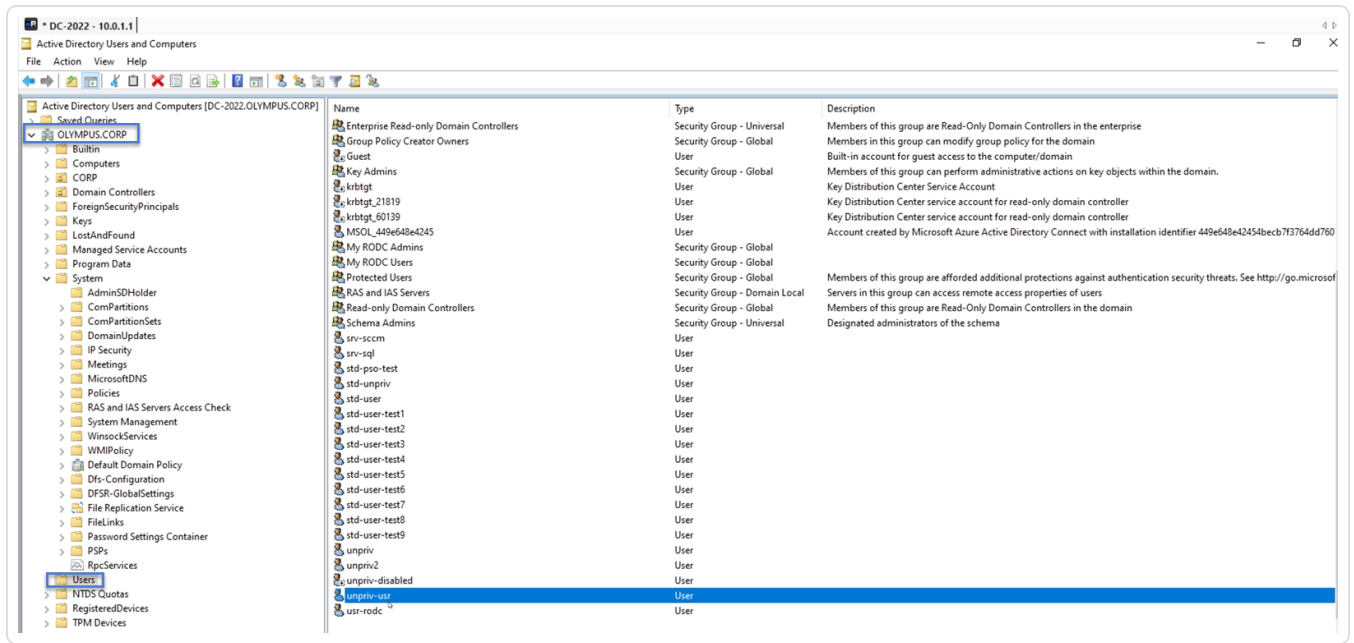
Tipo	Objeto	Ruta	Dominio	Motivos
LDAP	user	CN=Adan Abreu,OU=AlsId,DC=alsId,DC=corp	ALSID	Cuenta estándar con adminCount

Cuenta estándar con ADMINCOUNT 13:17:56, 2023-05-03

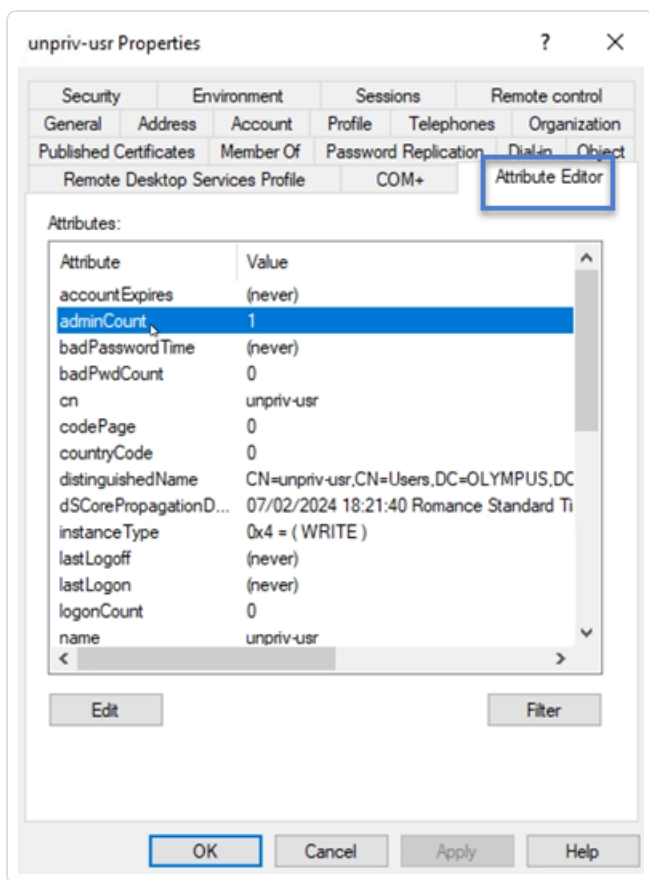
La cuenta Adan Abreu contiene un atributo adminCount, distinto de 0 y no pertenece a un grupo privilegiado en ALSID. Debido a este error, la cuenta omite medias estándar de control de acceso. En particular, la delegación de derechos de acceso aplicada a la jerarquía Adan Abreu no se aplica a Adan Abreu, lo que podría llevar a la aplicación incorrecta de políticas de seguridad en el objeto.

- En el Administrador de Escritorio remoto (o una herramienta similar), busque el nombre del dominio y navegue hasta **Usuarios** y la cuenta que Tenable Identity Exposure marcó.

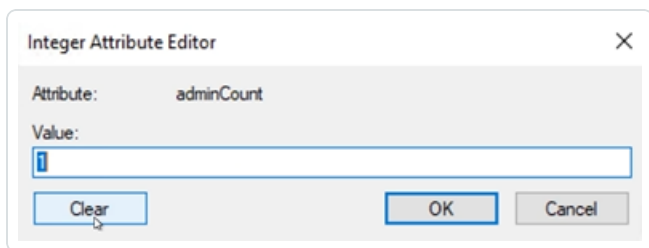
Permiso necesario: Para seguir el procedimiento, debe tener una cuenta de administrador en el dominio.



5. Haga clic en el nombre de la cuenta para abrir el cuadro de diálogo **Propiedades** y seleccione la pestaña **Editor de atributos**.
6. Desde la lista de atributos, haga clic en adminCount para abrir el cuadro de diálogo **Editor de atributos enteros**.



7. En el cuadro de diálogo, haga clic en **Borrar** y **Aceptar**.



8. En Tenable Identity Exposure, regrese al panel "Detalles del indicador" y actualice la página.

El objeto anómalo ya no aparece en la lista.

Delegación peligrosa de Kerberos.

El protocolo Kerberos, que es fundamental para la seguridad de Active Directory, permite que ciertos servidores reutilicen las credenciales de usuarios. Si un atacante pone en peligro uno de estos servidores, podría robar estas credenciales y usarlas para autenticarse en otros recursos.

Este IoE de nivel crítico informa todas las cuentas que tienen atributos de delegación y excluye las cuentas deshabilitadas. Los usuarios privilegiados no deben tener atributos de delegación. Para



proteger estas cuentas de usuario, agréguelas al grupo “Usuarios protegidos” o márkelas como “La cuenta es importante y no se puede delegar”.

Para agregar la cuenta al grupo “Usuarios protegidos”:

1. En Tenable Identity Exposure, haga clic en **Indicadores de exposición** en el panel de navegación para que se abra.

De manera predeterminada, Tenable Identity Exposure muestra solo los loE que contienen objetos anómalos.

2. Haga clic en el mosaico del loE **Delegación peligrosa de Kerberos**.

The screenshot shows the 'Indicadores de exposición' (Exposure Indicators) dashboard. It features a search bar at the top and a grid of 12 indicator cards. The 'Delegación peligrosa de Kerberos' (Dangerous Kerberos Delegation) indicator is highlighted with a mouse cursor. Other indicators include 'Controladores de dominio administrados por usuarios ilegítimos', 'Comprobar los permisos de objetos y archivos de GPO sensibles', 'Grupo principal de usuarios', 'Errores de configuración peligrosos de AD CS', 'Verificar los permisos relacionados con cuentas de Microsoft Entra Connect', 'Aplicación de políticas de contraseñas débiles en los usuarios', 'Permisos de objetos raíz que permiten ataques similares a DCSync', 'Cuentas con un atributo SID History peligroso', 'Asegurar la coherencia de SDProp', 'Miembros de grupos administrativos nativos', and 'Cuentas con privilegios que ejecutan servicios de Kerberos'.

Se abre el panel **Detalles del indicador**.

3. Pase el cursor por el objeto anómalo y haga clic en él para mostrar los detalles y anote el nombre del dominio y la cuenta. (En este ejemplo: Dominio = OLYMPUS.CORP y cuenta = adm-t0).

The screenshot shows the 'Detalles del indicador' (Indicator Details) panel for 'Delegación peligrosa de Kerberos'. The indicator is marked as 'Crítica' (Critical) and 'No cumple' (Not Compliant). The 'OBJETOS ANÓMALOS' (Anomalous Objects) table is visible, with the following data:

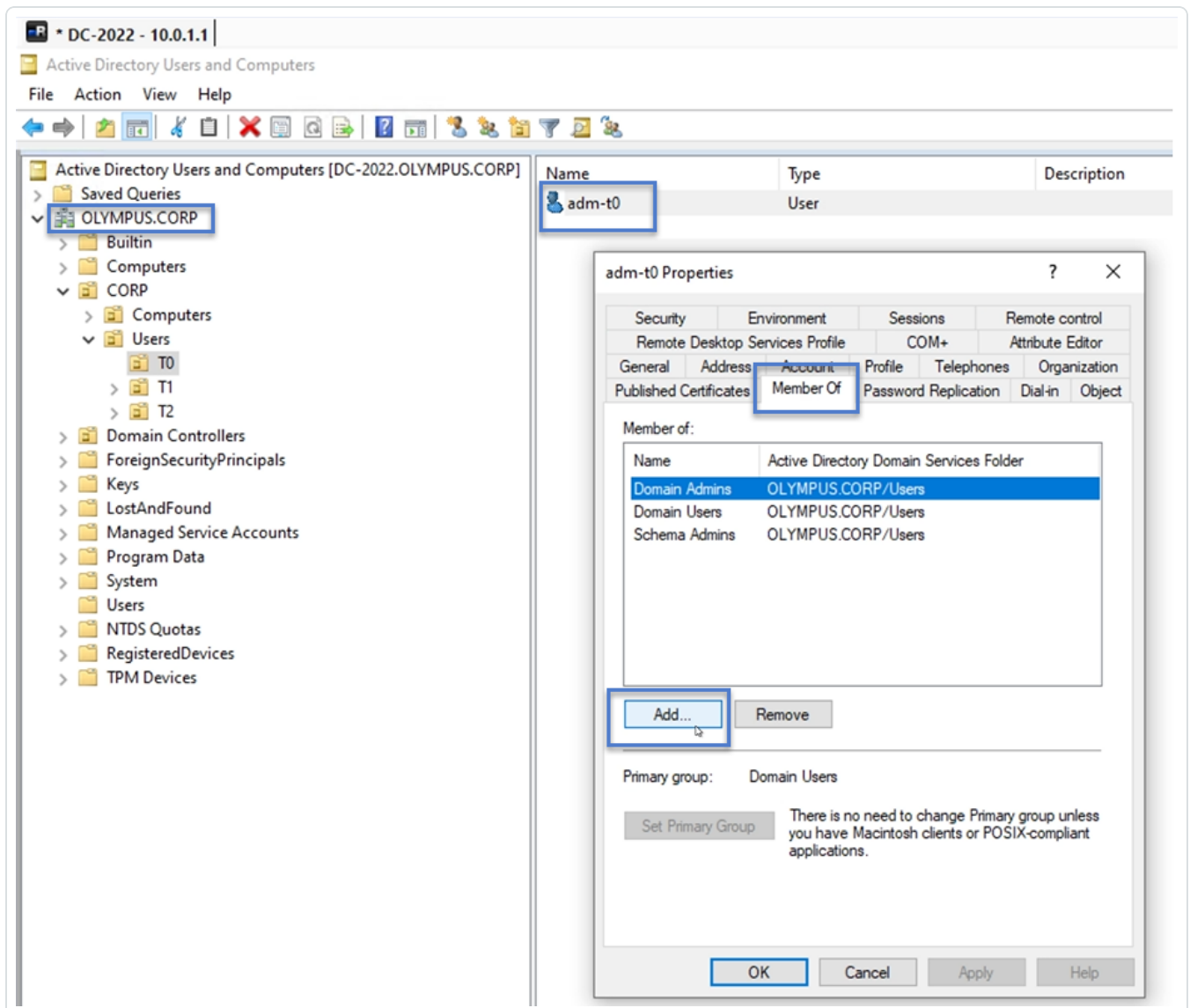
Tipo	Objeto	Ruta	Dominio	Motivos
LDAP	user	CN=localadmin,CN=Users,DC=jp,DC=alsid,DC=corp	Japan Domain @ Alsid corp	Sin protección frente a la delegación

Below the table, a detailed view of the selected object is shown. The text indicates that the account 'localadmin' is privileged and does not have the 'NOT_DELEGATED' attribute, which is a security concern. The detection date is 07-54-12, 2022-01-26.

- En el Administrador de Escritorio remoto (o una herramienta similar), busque el nombre del dominio y navegue hasta el dominio y la cuenta que Tenable Identity Exposure marcó.

Permiso necesario: Para seguir el procedimiento, debe tener una cuenta de administrador en el dominio.

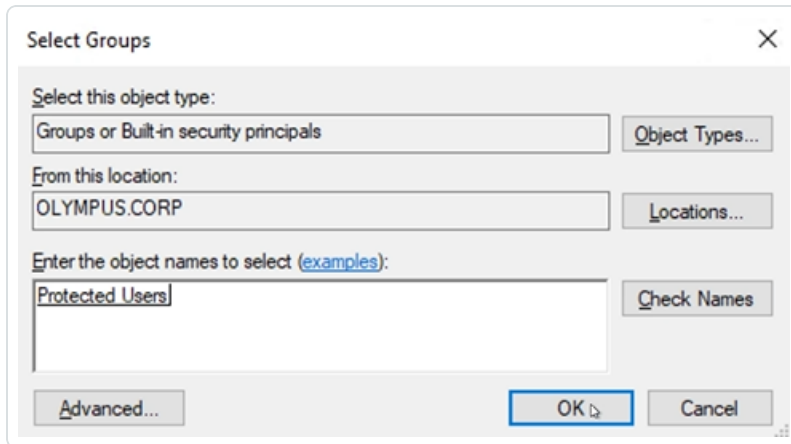
- Haga clic en el nombre de la cuenta para abrir el cuadro de diálogo **Propiedades** y seleccione la pestaña **Miembro de**.
- Desde la lista de miembros, haga clic en **Agregar**.



Aparece el cuadro de diálogo **Seleccionar grupos**.



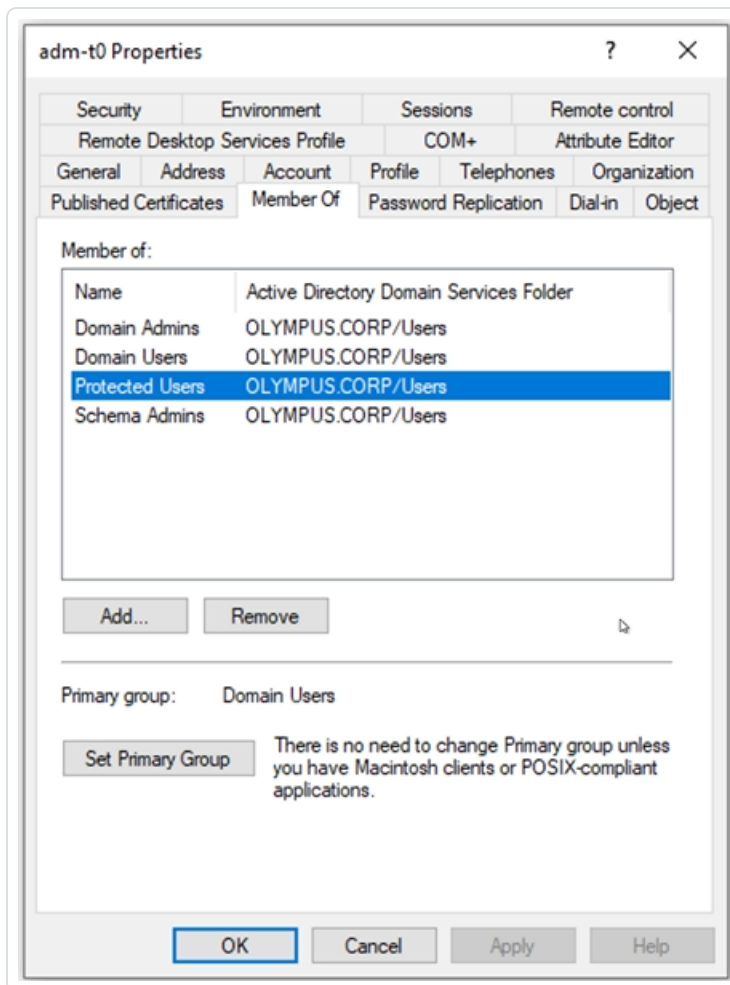
7. Escriba el nombre del objeto "Usuarios protegidos" y haga clic en **Comprobar nombres**.



8. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.

9. En el cuadro de diálogo **Propiedades**, haga clic en **Aplicar**.

El nuevo grupo aparece en la lista de miembros.



10. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
11. En Tenable Identity Exposure, regrese al panel “Detalles del indicador” y actualice la página.
El objeto anómalo ya no aparece en la lista.

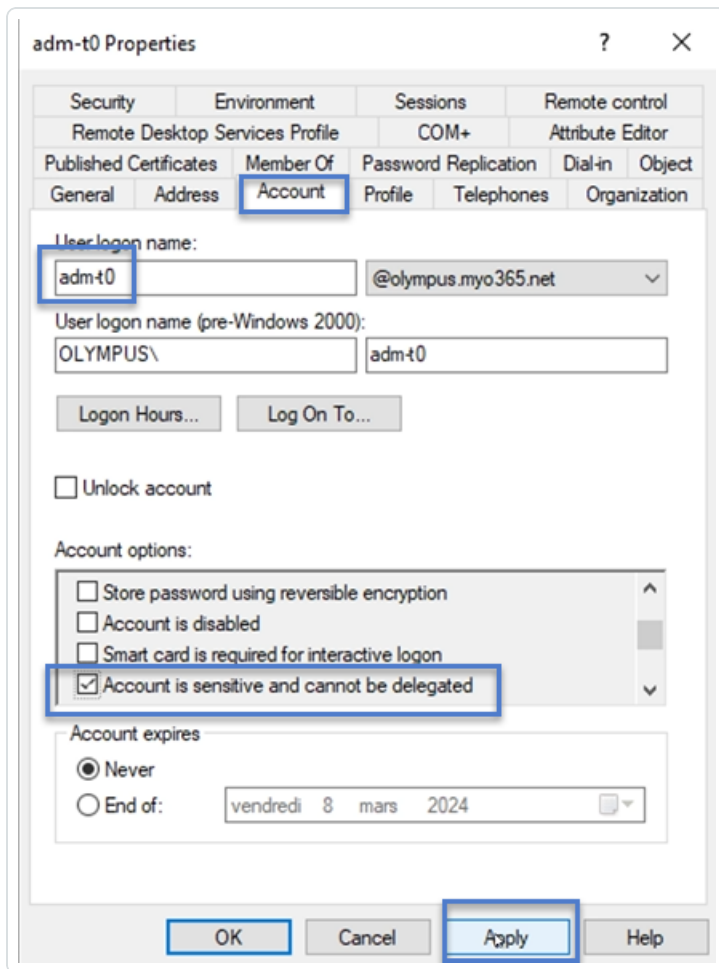
Para configurar la cuenta como “no se puede delegar”:

1. En el Administrador de Escritorio remoto, busque el nombre del dominio y navegue hasta el dominio y la cuenta que Tenable Identity Exposure marcó.

Permiso necesario: Para seguir el procedimiento, debe tener una cuenta de administrador en el dominio.

2. Haga clic en el nombre de la cuenta para abrir el cuadro de diálogo **Propiedades** y seleccione la pestaña **Cuenta**.

- De la lista de opciones de cuenta, seleccione “La cuenta es importante y no se puede delegar” y haga clic en **Aplicar**.



- Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
- En Tenable Identity Exposure, regrese al panel “Detalles del indicador” y actualice la página.

El objeto anómalo ya no aparece en la lista.

Asegurar la coherencia de SDProp.

Los atacantes que ponen un dominio de Active Directory en peligro suelen cambiar la ACL del objeto `adminSDHolder`, y todo permiso que agregan a la ACL se copia en los usuarios privilegiados, lo que facilita la configuración de puertas traseras.

Este IoE de nivel crítico comprueba que los permisos establecidos en el objeto `adminSDHolder` solo permitan acceso privilegiado a cuentas administrativas.

Para corregir un objeto anómalo del IoE **Asegurar la coherencia de SDProp**:



1. En Tenable Identity Exposure, haga clic en **Indicadores de exposición** en el panel de navegación para que se abra.

De manera predeterminada, Tenable Identity Exposure muestra solo los loE que contienen objetos anómalos.

2. Haga clic en el mosaico del loE **Asegurar la coherencia de SDProp**.

Se abre el panel **Detalles del indicador**.

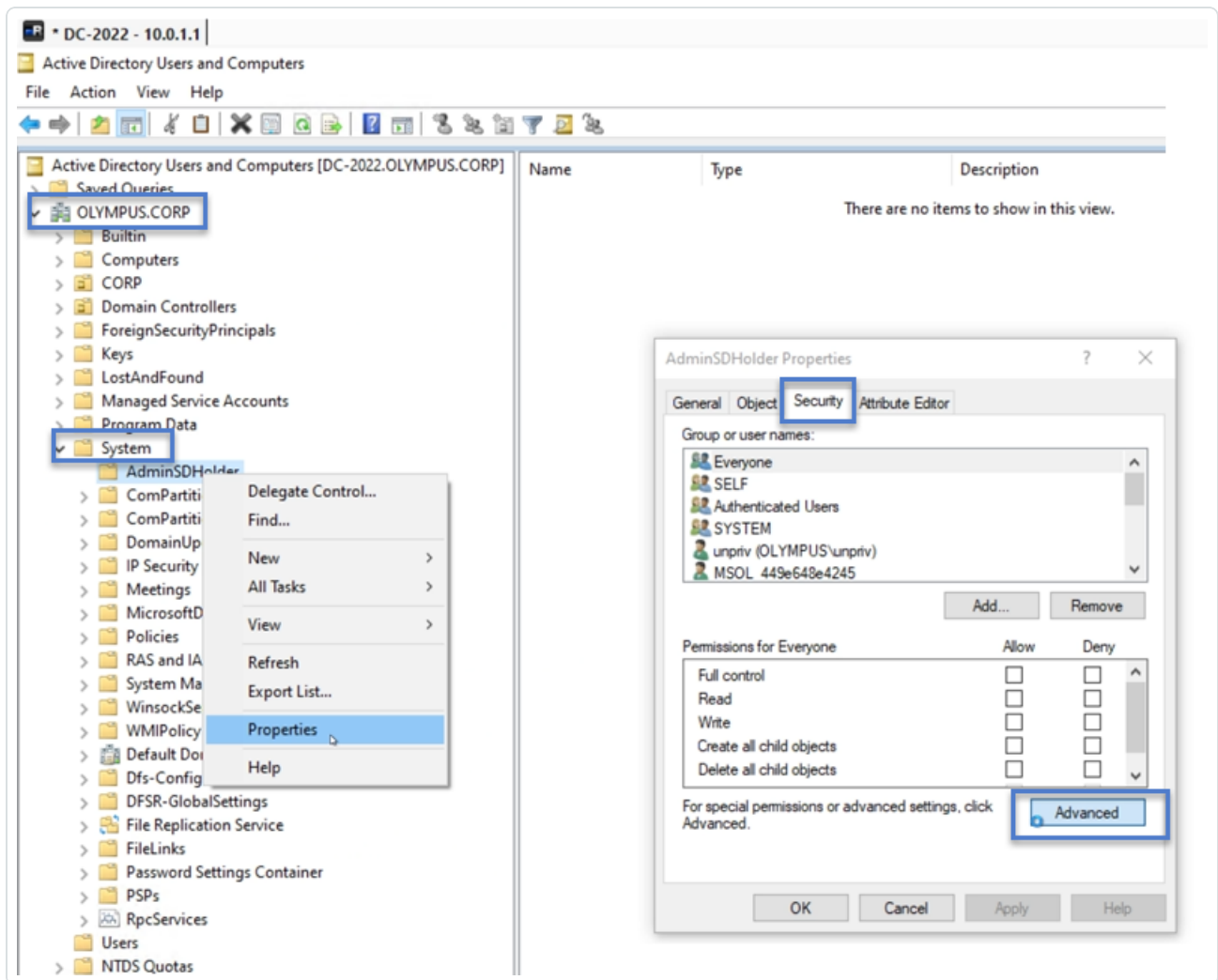
3. Pase el cursor por el objeto anómalo y haga clic en él para mostrar los detalles. Anote el nombre del dominio y el permiso asociado que Tenable Identity Exposure marcó. (En este ejemplo: OLYMPUS.CORP\unpriv).

The screenshot shows the Tenable Identity Exposure dashboard. At the top, there's a navigation bar with the Tenable logo and 'Identity Exposure'. Below it, a header for the alert 'Asegurar la coherencia de SDProp' is displayed, indicating a 'Crítica' (Critical) severity and 'No cumple' (Does not comply) status. The main content area is titled 'OBJETOS ANOMALOS' and contains a table with columns for Tipo, Objeto, Ruta, Dominio, and Motivos. A row is highlighted with a mouse cursor, showing 'LDAP' as the type, 'container' as the object, and 'CN=AdminSDHolder,CN=System,DC=alsid,DC=corp' as the path. Below the table, a section titled 'PERMISOS INSEGUROS EN ADMINSDHOLDER' provides details on the permissions, including a list of ACLs and their associated permissions like 'Write all properties' and 'All validated writes'.

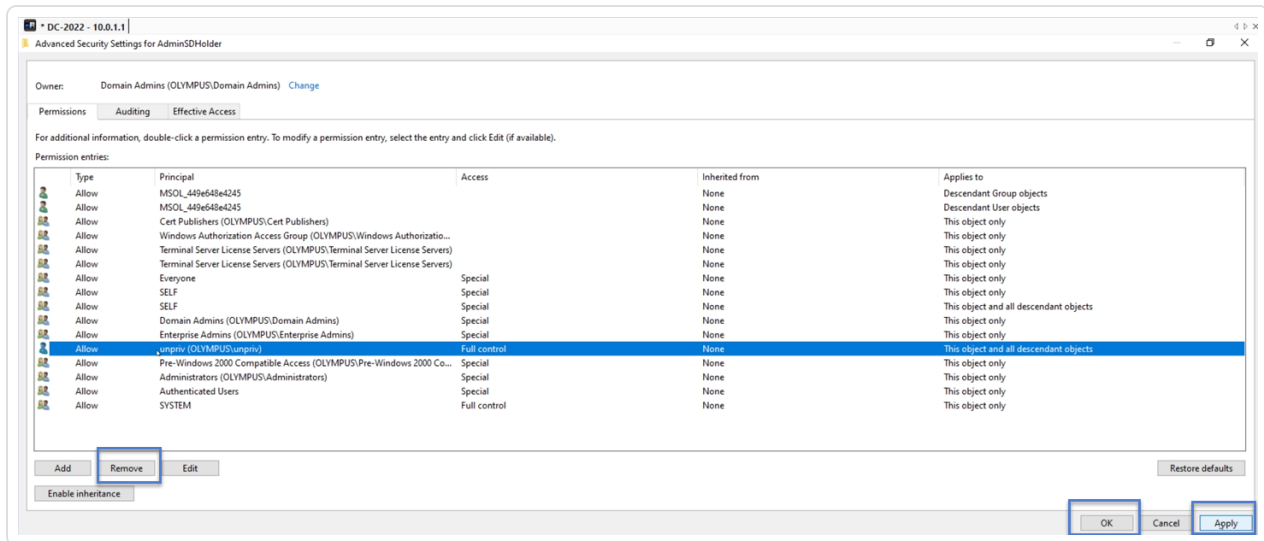
4. En el Administrador de Escritorio remoto (o una herramienta similar), busque el nombre del dominio y navegue hasta **Sistema > AdminSDHolder**.

Permiso necesario: Para seguir el procedimiento, debe tener una cuenta de administrador en el dominio.

5. Haga clic con el botón derecho en **AdminSDHolder** y seleccione **Propiedades** en el menú contextual.



6. En el cuadro de diálogo **Propiedades**, seleccione la pestaña **Seguridad** y haga clic en **Opciones avanzadas**.
7. En la ventana **Configuración de seguridad avanzada** y en la pestaña **Permisos**, seleccione de la lista de entradas de permisos el que haya generado la alerta.
8. Haga clic en **Quitar**.
9. Haga clic en **Aplicar** y en **Aceptar** para cerrar la ventana de configuración.
10. Haga clic en **Aceptar** para cerrar la ventana **Propiedades**.



11. En Tenable Identity Exposure, regrese al panel “Detalles del indicador” y actualice la página. El objeto anómalo ya no aparece en la lista.

Indicadores de ataque

Licencia necesaria: indicadores de ataque

Los **indicadores de ataque** (IoA) de Tenable Identity Exposure le brindan la capacidad de detectar ataques a su instancia de Active Directory (AD).

Una vista consolidada de los indicadores de ataque muestra en un solo panel una línea temporal, los tres principales incidentes que afectaron a su instancia de AD en tiempo real y la distribución de ataques. Puede hacer lo siguiente:

- Visualizar cada amenaza a partir de una línea temporal de ataques precisa.
- Analizar en profundidad los detalles de un ataque a la instancia de AD.
- Explorar las descripciones de MITRE ATT&CK directamente a partir de los incidentes detectados.

Para obtener más información sobre IoA específicos, consulte la [Guía de referencia de indicadores de ataque](#) (requiere iniciar sesión en el sitio de descargas de Tenable).

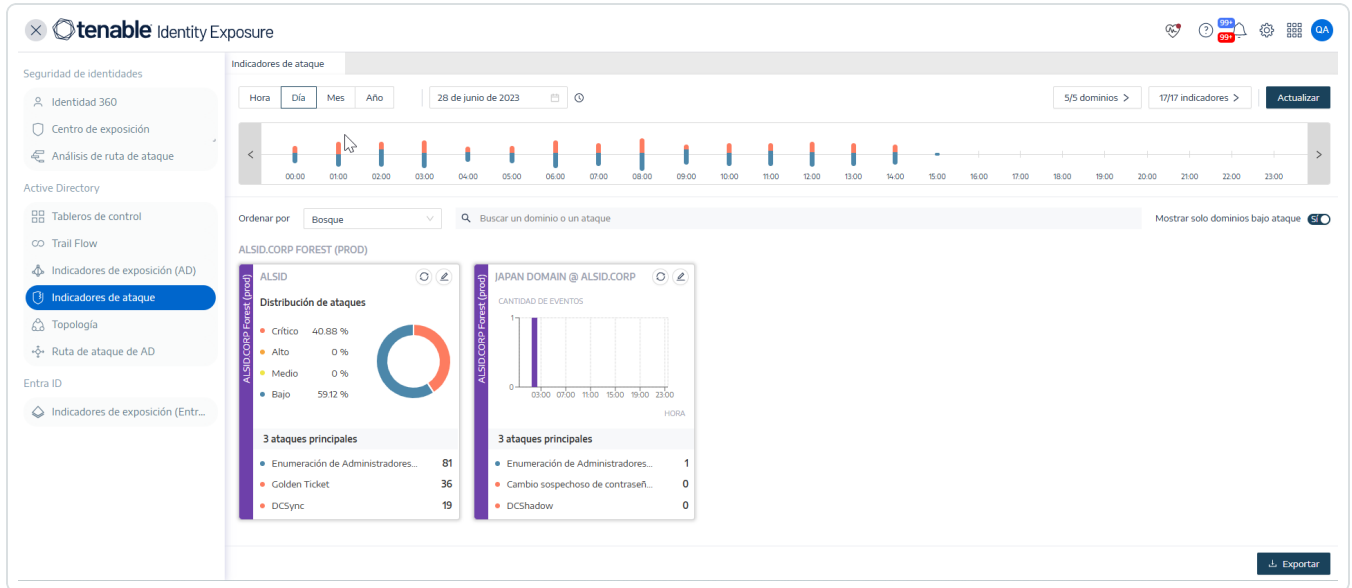
Nota: Si se detectaron una gran cantidad de ataques, verifique que el administrador haya aplicado los valores recomendados para las distintas opciones de los indicadores de ataque para calibrar correctamente los IoA. Para obtener más información, consulte [Para calibrar los IoA](#).




Para mostrar los indicadores de ataque:

1. En Tenable Identity Exposure, haga clic en **Indicadores de ataque** en el panel de navegación.

Se abre el panel **Indicadores de ataque**.



2. De manera predeterminada, Tenable Identity Exposure muestra todos sus bosques y dominios de AD. Para ajustar esta vista, siga cualquiera de los procedimientos a continuación:

- Seleccione el período de tiempo que quiere mostrar: haga clic en **Hora**, **Día** (predeterminado), **Mes** o **Año**.
- Muévase por la línea temporal: haga clic en la flecha izquierda o derecha para avanzar o retroceder en la línea temporal.
- Seleccione una hora en particular: haga clic en el selector de fechas para elegir una hora, un día, un mes o un año.
- Regrese a la fecha y hora actuales: haga clic en el ícono  junto al selector de fechas.
- Seleccione los dominios: haga clic en **n/n dominios**.
 - a. En el panel **Bosques y dominios**, seleccione los dominios.
 - b. Haga clic en **Filtrar selección**.



Tenable Identity Exposure actualiza la vista.

- Seleccione los loA: haga clic en **n/n indicadores**.
 - a. En el panel “Indicadores de ataque”, seleccione los loA.
 - b. Haga clic en **Filtrar selección**.

Tenable Identity Exposure actualiza la vista.

- Ordene los mosaicos de los loA: en el cuadro **Ordenar por**, haga clic en la flecha para mostrar una lista desplegable de opciones: **Dominio**, **Criticidad** o **Bosque**.
- Busque un dominio o ataque: en el cuadro **Buscar**, escriba el nombre del dominio o del ataque.
- Muestre solo los dominios bajo ataque: haga clic en el conmutador **Mostrar solo dominios bajo ataque** para establecerlo en **Sí**.
- Exporte un informe de ataques: haga clic en **Exportar**.

Aparece el panel **Exportar tarjetas**.

- a. En el cuadro **Formato de exportación**, haga clic en la flecha de la lista desplegable para seleccionar un formato: **PDF**, **CSV** o **PPTX**.
- b. Haga clic en **Exportar**.

Tenable Identity Exposure descarga el informe en la máquina local.

Nivel de gravedad

Tenable Identity Exposure detecta y asigna niveles de gravedad a los ataques:

Nivel	Descripción
Crítico: rojo	Se detectó un ataque posterior a la explotación probado que requiere la dominación del dominio como requisito previo.
Alto: naranja	Se detectó un ataque importante que permite que un atacante logre la dominación del dominio.
Medio: amarillo	El loA se relaciona con un ataque que podría conducir a un escalamiento peligroso de privilegios o permitir el acceso a recursos confidenciales.



Bajo: azul

Alerta sobre comportamientos sospechosos relacionados con acciones de reconocimiento o incidentes de bajo impacto.

Consulte también

- [Detalles de un indicador de ataque](#)
- [Incidentes de indicadores de ataque](#)

Detalles de un indicador de ataque

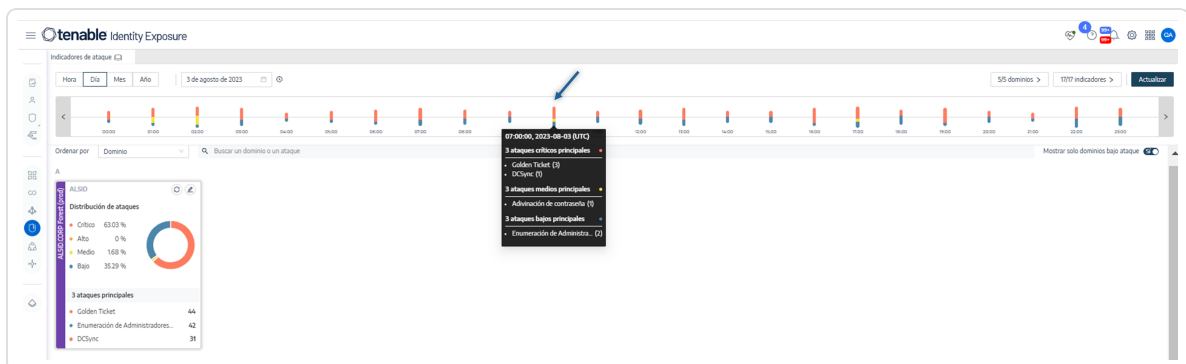
En el panel “Indicadores de ataque” de Tenable Identity Exposure se muestra información sobre los ataques que tuvieron lugar en su instancia de Active Directory.

Para ver los indicadores de ataque:

- En Tenable Identity Exposure, haga clic en **Indicadores de ataque** en el panel de navegación. Se abre el panel **Indicadores de ataque**.

Para mostrar información del ataque en la línea temporal:

- Haga clic en cualquier evento de la línea temporal para mostrar:
 - La fecha y hora de detección del incidente.
 - El nivel de gravedad de los tres ataques principales.
 - La cantidad total de ataques detectados en esta fecha y hora.



Para cambiar el tipo de gráfico:

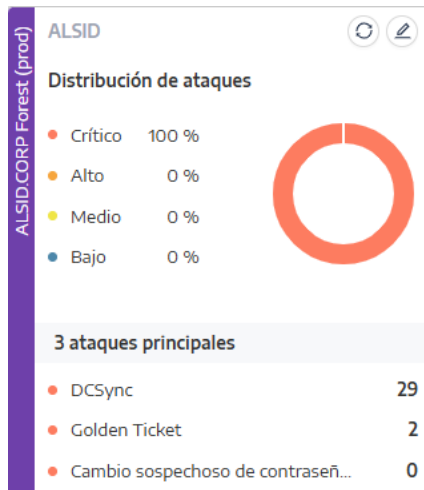


1. Haga clic en el ícono  para editar el mosaico del dominio.

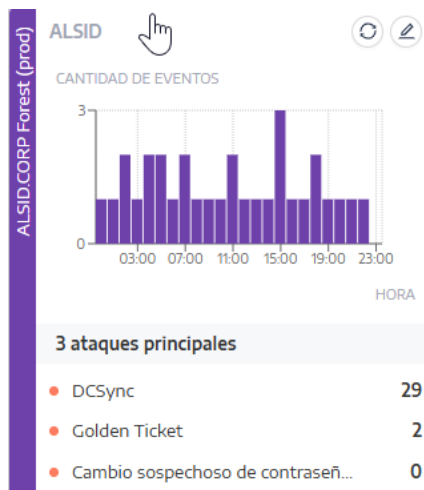
Aparece el panel **Editar información de la tarjeta**.

2. Seleccione un tipo de gráfico:

- **Distribución de ataques:** muestra la distribución de la gravedad de los ataques.



- **Cantidad de eventos:** muestra los tres ataques principales y la cantidad de veces que ocurrieron.



3. Haga clic en **Guardar**.

Tenable Identity Exposure actualiza el gráfico.

Consulte también



- [Indicadores de ataque](#)
- [Incidentes de indicadores de ataque](#)

Incidentes de indicadores de ataque

La lista de incidentes de los indicadores de ataque (IoA) brinda información detallada sobre ataques específicos a su instancia de Active Directory (AD). Esto le permite adoptar la medida necesaria según el nivel de gravedad del IoA.

Para ver los incidentes de ataque:

1. En Tenable Identity Exposure, haga clic en **Indicadores de ataque** en el panel de navegación.

Se abre el panel **Indicadores de ataque**.

2. Haga clic en el mosaico de cualquier dominio.

Aparece el panel **Lista de incidentes** con una lista de incidentes que tuvieron lugar en el dominio.

La cuenta de sneaky@alsid.corp se usó para iniciar un ataque DCSync. Es posible que algunos secretos críticos de AD se hayan sincronizado durante el ataque. El ataque se lanzó desde la máquina AP3LAB-TOOLS (10.200.200.5) y se dirigió a dc-vim (10.0.0.234).

Fecha	Nombre del ataque	Dominio
2024-11-17 22:05:13	DCSync	ALSID.CORP Forest (prod)
2024-11-17 21:18:13	DCSync	ALSID.CORP Forest (prod)
2024-11-17 20:38:13	DCSync	ALSID.CORP Forest (prod)
2024-11-17 19:44:13	DCSync	ALSID.CORP Forest (prod)
2024-11-17 18:57:13	DCSync	ALSID.CORP Forest (prod)
2024-11-17 18:10:13	DCSync	ALSID.CORP Forest (prod)
2024-11-17 17:23:13	DCSync	ALSID.CORP Forest (prod)

3. Desde esta lista, puede realizar cualquiera de las siguientes acciones:

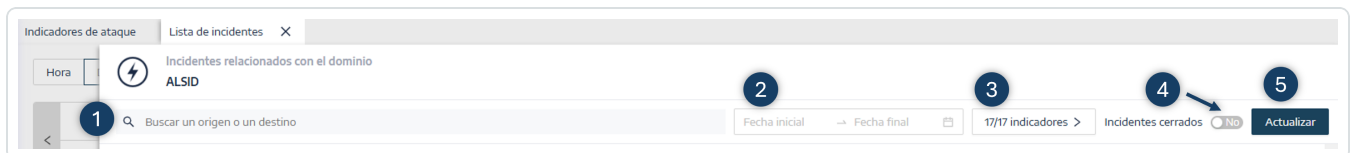


- Definir criterios de búsqueda para buscar incidentes específicos **(1)**.
- Acceder a explicaciones detalladas sobre los ataques que afectan a la instancia de AD **(2)**.
- Cerrar o reabrir un incidente **(3)**.
- Descargar un informe en el que se muestren todos los incidentes **(4)**.

Para buscar un incidente:

1. En el cuadro **Buscar**, escriba el nombre de un origen o destino.
2. Haga clic en el selector de fechas para seleccionar una fecha inicial y una fecha final para el incidente.
3. Haga clic en **n/n indicadores** para seleccionar los indicadores relacionados.
4. Haga clic en el conmutador **Incidentes cerrados** para establecerlo en **Si** y limitar la búsqueda a los incidentes cerrados.
5. Haga clic en **Actualizar**.

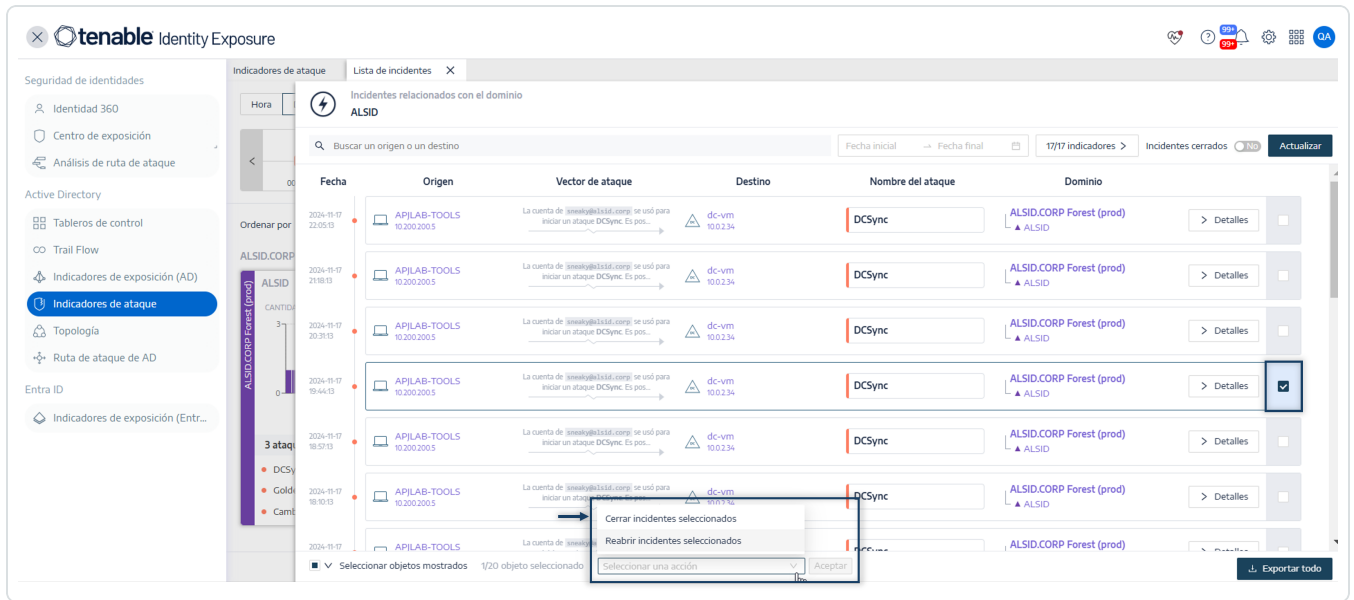
Tenable Identity Exposure actualiza la lista con los incidentes correspondientes.



Para cerrar un incidente:



1. De la lista de incidentes, seleccione un incidente para cerrarlo o reabrirlo.



2. Al final del panel, haga clic en el menú desplegable y seleccione **Cerrar incidentes seleccionados**.

3. Haga clic en **Aceptar**.

Aparece un mensaje para pedirle que confirme el cierre.

4. Haga clic en **Confirmar**.

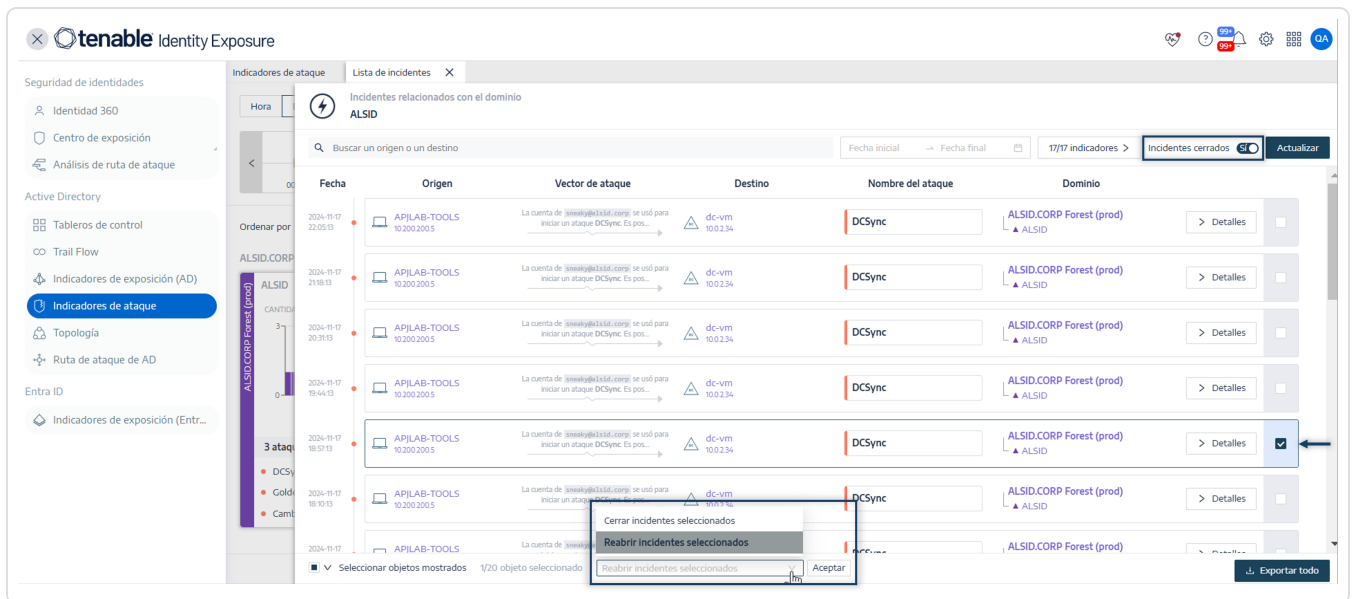
Un mensaje confirma que Tenable Identity Exposure cerró el incidente y ya no lo muestra.

Para reabrir un incidente:

1. En el panel **Lista de incidentes**, haga clic en el conmutador **Incidentes cerrados** para establecerlo en **Sí**.

Tenable Identity Exposure actualiza la lista con los incidentes cerrados.

2. Seleccione el incidente que quiere reabrir.



3. Al final del panel, haga clic en el menú desplegable y seleccione **Reabrir incidentes seleccionados**.

4. Haga clic en **Aceptar**.

Un mensaje confirma que Tenable Identity Exposure reabrió el incidente.

Sugerencia: Puede cerrar o reabrir incidentes en masa. Al final del panel, haga clic en **Seleccionar objetos mostrados**.

Para exportar incidentes

1. En el panel **Lista de incidentes**, haga clic en el botón **Exportar todo** en la parte inferior.

Se abre el panel lateral **Exportar incidentes**.

2. En el cuadro de lista desplegable **Separador**, seleccione un separador para los datos exportados: **coma** o **punto y coma**.

Tenable Identity Exposure exporta los datos en formato CSV para su descarga.



Detalles del incidente

En cada entrada de la lista de incidentes se muestra la siguiente información:

- **Fecha:** la fecha en que ocurrió el incidente que desencadenó el loA. Tenable Identity Exposure muestra los más recientes al principio de la línea temporal.
- **Origen:** el origen de donde provino el ataque y su dirección IP.
- **Vector de ataque:** una explicación sobre lo que sucedió durante el ataque.

Sugerencia: Pase el cursor por el vector de ataque para ver más información sobre el loA.

- **Destino:** el objetivo del ataque y su dirección IP.
- **Nombre del ataque:** el nombre técnico del ataque.
- **Dominio:** los dominios a los que afectó el ataque.

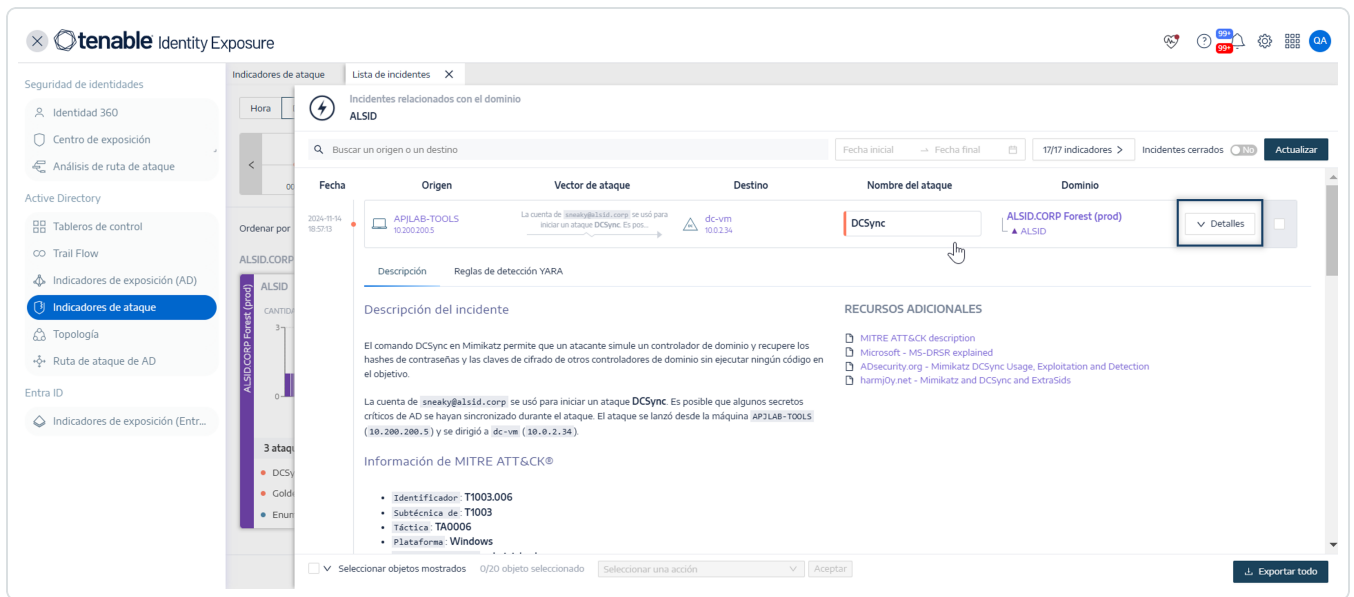
Sugerencia: Tenable Identity Exposure puede mostrar un máximo de cinco paneles al hacer clic en varios elementos interactivos (vínculos, botones de acción, etc.) en la **Lista de incidentes**. Para cerrar todos los paneles a la vez, haga clic en cualquier lugar de la página.

Detalles del ataque

Desde la lista de incidentes, puede explorar en profundidad un ataque específico y tomar las medidas necesarias para corregirlo.

Para mostrar los detalles de un ataque:

1. De la lista de incidentes, seleccione un incidente para explorar los detalles.
2. Haga clic en **Detalles**.



Tenable Identity Exposure muestra los detalles asociados a ese ataque:

Descripción

La pestaña **Descripción** contiene las siguientes secciones:

- **Descripción del incidente:** ofrece una breve descripción del ataque.
- **Información de MITRE ATT&CK:** brinda información técnica recuperada de la base de conocimientos de Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). Mitre Att&ck es un marco que clasifica los ataques de adversarios y describe las acciones que toman los atacantes después de poner una red en peligro. También proporciona identificadores estándar para vulnerabilidades de seguridad con el fin de asegurar que la comunidad de la ciberseguridad comparta criterios.
- **Recursos adicionales:** se ofrecen vínculos a sitios web, artículos y documentos técnicos para obtener información más detallada sobre el ataque.

Reglas de detección YARA

En la pestaña **Reglas de detección YARA** se describen las reglas YARA que Tenable Identity Exposure usa para detectar ataques a AD en el nivel de la red para fortalecer la cadena de detección de Tenable Identity Exposure.



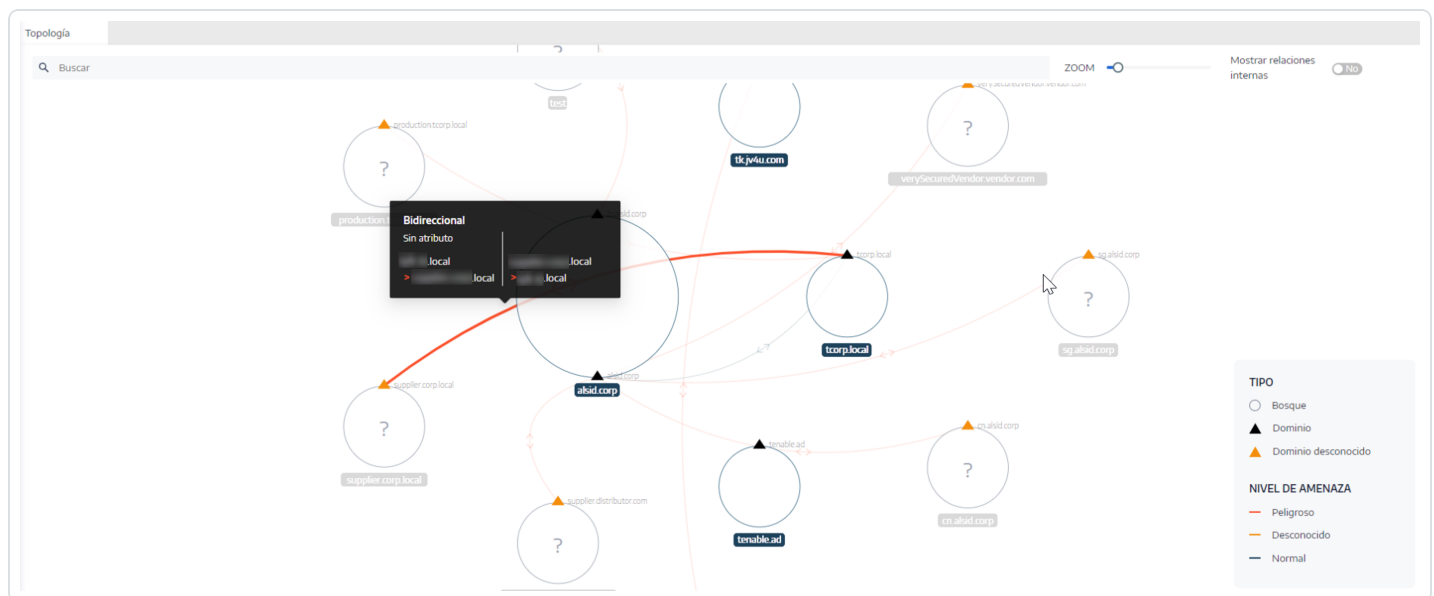
Nota: YARA es el nombre de una herramienta usada principalmente en la investigación y detección de malware. Proporciona un sistema basado en reglas para crear descripciones de familias de malware en función de patrones textuales o binarios. En esencia, una descripción es el nombre de una regla YARA, donde estas reglas constan de conjuntos de cadenas y una expresión booleana (fuente: wikipedia.org).

Consulte también

- [Indicadores de ataque](#)
- [Detalles de un indicador de ataque](#)

Topología

En la página “Topología” se ofrece una visualización gráfica interactiva de la instancia de Active Directory. En el **gráfico de la topología**, se muestran los bosques, los dominios y las relaciones de confianza que existen entre ellos.



Para abrir la página “Topología”:

- En Tenable Identity Exposure, haga clic en **Topología** en el menú de navegación de la izquierda.

El panel “Topología” se abre con una representación gráfica de la instancia de AD.

Para buscar un dominio:



- En el panel **Topología**, escriba el nombre de un dominio en el cuadro **Buscar**.

Tenable Identity Exposure resalta el dominio.

Para ampliar el gráfico:

- En el panel **Topología**, haga clic en el control deslizante **Zoom** para ajustar el tamaño del gráfico.

Para mostrar el vínculo entre dos dominios:

- En el panel **Topología**, haga clic en el conmutador **Mostrar relaciones internas** para establecerlo en **Sí**.

Para mostrar los detalles sobre un dominio:

- En el panel **Topología**, haga clic en  para el nombre del dominio.

Se abre el panel **Detalles del dominio** con los indicadores de exposición (IoE) detectados y la puntuación de cumplimiento del dominio. Puede hacer clic en el mosaico del IoE para obtener más información.

Consulte también

- [Relaciones de confianza](#)
- [Relaciones de confianza peligrosas](#)

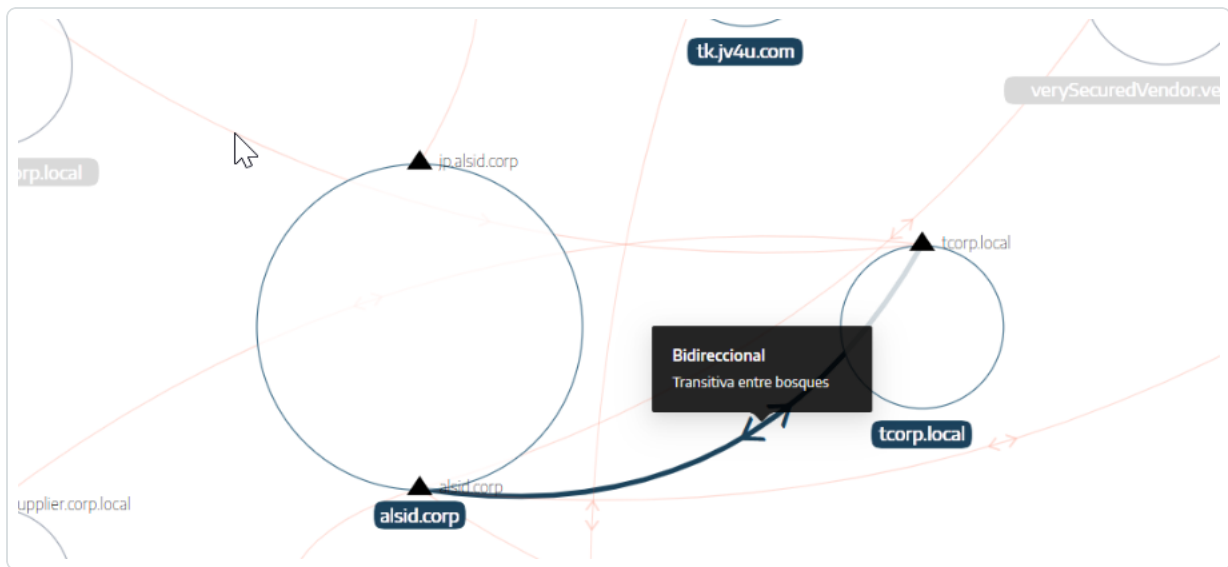
Relaciones de confianza

Las flechas curvas entre dominios en el gráfico de la topología representan relaciones de confianza.

Para mostrar las relaciones de confianza:

- En el gráfico de la topología, pase el cursor por las flechas curvas.

Tenable Identity Exposure muestra las relaciones de confianza con los atributos específicos entre dos entidades.



El color de una relación de confianza depende de su nivel de amenaza:

- **Rojo** para relaciones de confianza peligrosas
- **Naranja** para relaciones de confianza normales
- **Azul** para relaciones de confianza desconocidas

Para obtener más información, consulte [Relaciones de confianza peligrosas](#).

La información del atributo de confianza indica la dirección de la relación de confianza como **unidireccional** o **bidireccional** (entrante/saliente) y muestra uno de los siguientes valores:

Valor	Descripción
No transitiva	De manera predeterminada, las relaciones de confianza dentro del bosque son relaciones transitivas. Tenable Identity Exposure usa esta marca para convertirlas en relaciones de confianza no transitivas. Por otro lado, las relaciones de confianza entre bosques no son transitivas de manera predeterminada, de ahí la presencia de la marca de transitividad entre bosques. Tenable Identity Exposure muestra este valor si existe una relación de confianza entre dominios dentro del bosque. La relación de confianza no concede acceso ni delega autoridad a dominios interconectados más allá del bosque.
Transitiva entre bosques	Indica que existe una relación de confianza transitiva entre dos bosques. La relación de confianza otorgada a otro dominio puede pasar al bosque



	de confianza.
Dentro del bosque	Indica que existe una relación de confianza entre dominios dentro del mismo bosque. Si tanto <code>WITHIN_FOREST</code> como <code>QUARANTINED_DOMAIN</code> están presentes, la relación de confianza se denomina QuarantinedWithinForest .
Solo nivel superior	Indica que solo los clientes que ejecutan sistemas operativos Windows 2000 y posteriores pueden utilizar esta relación de confianza.
Tratar como externa	(Solo cuando se aplica <code>FOREST_TRANSITIVE</code>) Indica un tipo externo de relación de confianza. Tenable Identity Exposure modifica el filtrado por identificador de seguridad (SID) en la relación de confianza y autoriza a pasar por el bosque a los SID cuyo identificador relativo (RID) sea mayor o igual que 1000.
En cuarentena	Indica que Tenable Identity Exposure habilitó el filtrado de los SID cuyo RID sea mayor o igual que 1000 para la relación de confianza. De manera predeterminada, Tenable Identity Exposure solo lo habilita para una relación de confianza externa, pero también puede aplicarse a una relación de confianza principal/secundaria o a una confianza de bosque.
Autenticación entre organizaciones	Indica que Tenable Identity Exposure habilitó la autenticación selectiva y puede usarla en relaciones de confianza de dominio o bosque.
Autenticación selectiva	Consulte Autenticación entre organizaciones.
Entre organizaciones sin delegación de TGT	Muestra si la delegación en un dominio de confianza está completamente deshabilitada (nunca establece la opción <code>ok-as-delegate</code> en los tickets de servicio emitidos).
Cifrado RC4	Indica que la relación de confianza admite claves de cifrado RC4 para intercambios de Kerberos. Esta marca está presente solo si <code>trustType</code> se aplica a <code>TRUST_TYPE_MIT</code> .
Claves de AES	Indica que la relación de confianza admite claves de cifrado AES para intercambios de Kerberos.



Confianza de PIM	Si se aplican las marcas FOREST_TRANSITIVE y TREAT_AS_EXTERNAL y la marca QUARANTINED_DOMAIN no está activada, la marca de relación de confianza de PIM indica que el bosque de confianza gestiona las identidades privilegiadas (gestión de identidades privilegiadas) con respecto al filtrado de SID (los SID locales pueden pasar por esta relación de confianza). La relación de confianza de PIM sirve para implementar bosques bastión.
Sin atributo	Indica que la relación de confianza externa no tiene ningún atributo específico.

Relaciones de confianza peligrosas

El color de una relación de confianza depende de su nivel de amenaza:

- **Rojo** para relaciones de confianza peligrosas
- **Naranja** para relaciones de confianza normales
- **Azul** para relaciones de confianza desconocidas

Para investigar una relación de confianza peligrosa:

1. En el gráfico de la topología, haga clic en las flechas curvas.

Se abre el panel **Objetos anómalos relativos a relaciones de confianza**.

Sugerencia: Los detalles de los eventos que se muestran en este panel de relaciones de confianza peligrosas están todos vinculados al indicador de exposición **Relaciones de confianza peligrosas**, al que también puede acceder desde el menú de navegación **Indicadores de exposición**.



Objetos anómalos relativos a relaciones de confianza

Nombre: Relaciones de confianza peligrosas | Gravedad: Alta | Estado: No cumple | Detección más reciente: No hay anomalías en esta etapa

OBJETOS ANÓMALOS

Tipo	Objeto	Ruta	Dominio	Motivos
LDAP	trustedDomain	CN=test,CN=System,DC=hp,DC=alsid,DC=corp	Japan Domain @ Alsid corp	Filtrado de identificadores de seguridad no habilitado
LDAP	trustedDomain	CN=supplier.distributor.com,CN=System,DC=alsid,DC=corp	ALSID	Filtrado de
LDAP	trustedDomain	CN=verySecuredVendor.vendor.com,CN=System,DC=alsid,DC=corp	ALSID	Filtrado de
LDAP	trustedDomain	CN=supplier.corp.local,CN=System,DC=tcorp,DC=local	TCORP Domain	Filtrado de
LDAP	trustedDomain	CN=production.tcorp.local,CN=System,DC=tcorp,DC=local	TCORP Domain	Filtrado de
LDAP	trustedDomain	CN=partner.contoso.com,CN=System,DC=tk,DC=jv4u,DC=com	TKJV4U	Filtrado de

2. Pase el cursor por un objeto anómalo de la lista y haga clic en él para mostrar los detalles.

Para exportar objetos anómalos:

1. En el gráfico de la topología, haga clic en las flechas curvas.

Se abre el panel **Objetos anómalos relativos a relaciones de confianza**.

2. Haga clic en **Exportar todo**.

Se abre el panel **Exportar objetos anómalos**.

3. En el cuadro **Formato de exportación**, haga clic en la flecha desplegable para seleccionar un formato.

4. Haga clic en **Exportar todo**.

Tenable Identity Exposure descarga en el equipo un archivo en el formato seleccionado.

5. Haga clic en la **X** para cerrar el panel.

Ruta de ataque

Tenable Identity Exposure ofrece varias maneras de visualizar la vulnerabilidad potencial de un activo empresarial a través de representaciones gráficas.



- **Ruta de ataque:** muestra las posibles rutas que puede tomar un atacante para poner en riesgo un activo desde un punto de entrada.
- **Radio de ataque:** muestra los posibles movimientos laterales en la instancia de Active Directory desde cualquier activo.
- **Exposición de los activos:** muestra todas las rutas que potencialmente pueden tomar el control de un activo.

Comprender la ruta de ataque le permitirá detectar los pasos de mitigación necesarios para evitar que los atacantes exploten las vulnerabilidades. Esto podría implicar la colocación de parches en los sistemas, el endurecimiento de las configuraciones, la implementación de controles de acceso más estrictos o la generación de conciencia entre los usuarios.

Beneficios de utilizar las rutas de ataque en Tenable Identity Exposure:

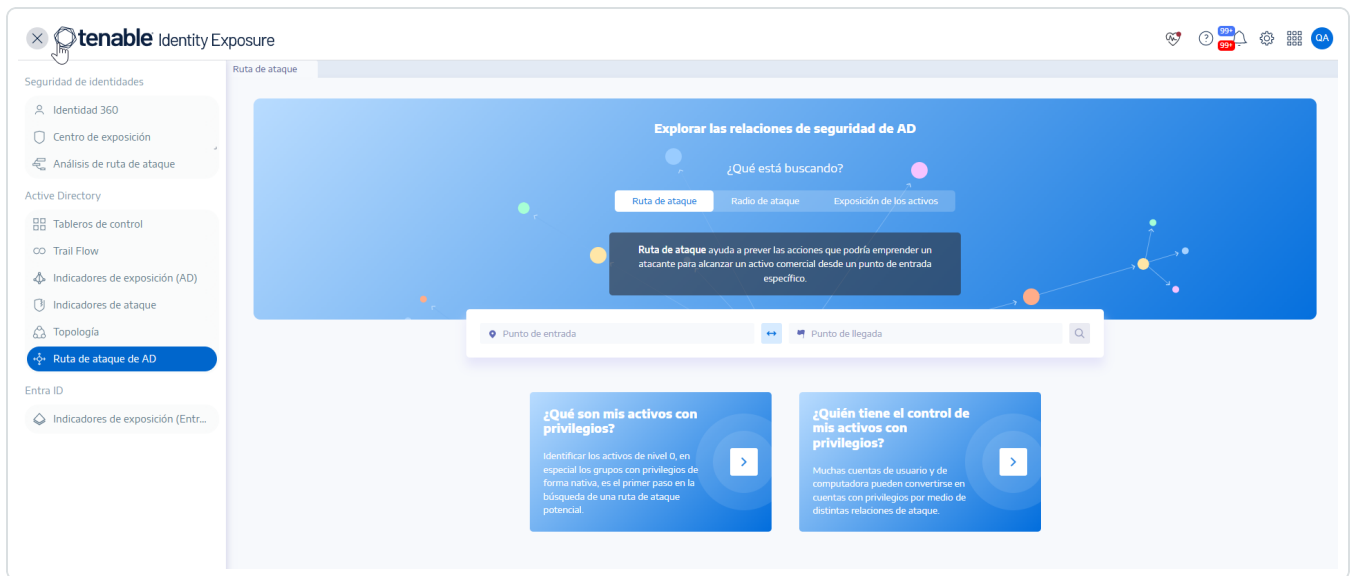
- **Seguridad proactiva:** ayuda a prever y abordar posibles vectores de ataque antes de que se exploten.
- **Priorización:** orienta a centrar los esfuerzos de seguridad en las vulnerabilidades y rutas de ataque más críticas.
- **Visualización:** ofrece una representación clara y fácil de entender de las relaciones de seguridad complejas dentro de la instancia de AD.
- **Comunicación:** facilita la comunicación de los riesgos de seguridad a las partes interesadas al ofrecer evidencia visual de posibles escenarios de ataque.


Para mostrar la ruta de ataque:

Especifique el punto de entrada, que podría ser cualquier activo de la instancia de AD (por ejemplo, una cuenta de usuario, un equipo o un grupo). Defina el punto de llegada, que representa el activo que el atacante pretende poner en peligro en última instancia (por ejemplo, un controlador de dominio o un servidor de datos confidenciales).

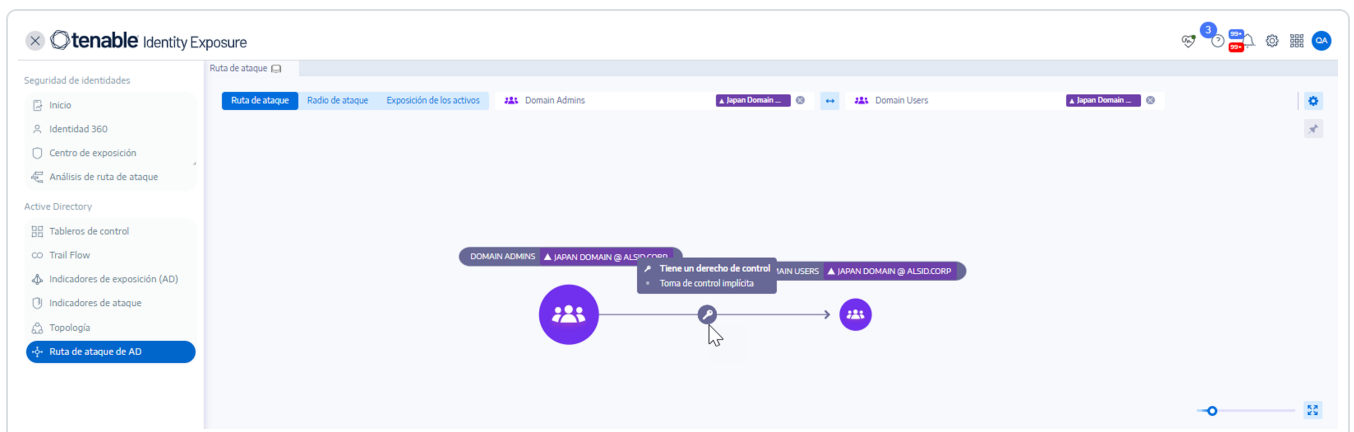
1. En Tenable Identity Exposure, haga clic en **Ruta de ataque** en el menú de la barra lateral.


Aparece el panel **Ruta de ataque**.



2. En el banner, haga clic en **Ruta de ataque**.
3. En el cuadro **Punto de entrada**, escriba el activo del punto de entrada.
4. En el cuadro **Punto de llegada**, escriba el activo del final de la ruta.
5. Haga clic en el ícono .

Tenable Identity Exposure muestra la ruta de ataque entre los dos activos.




6. De manera opcional, puede hacer clic en el ícono  para lo siguiente:



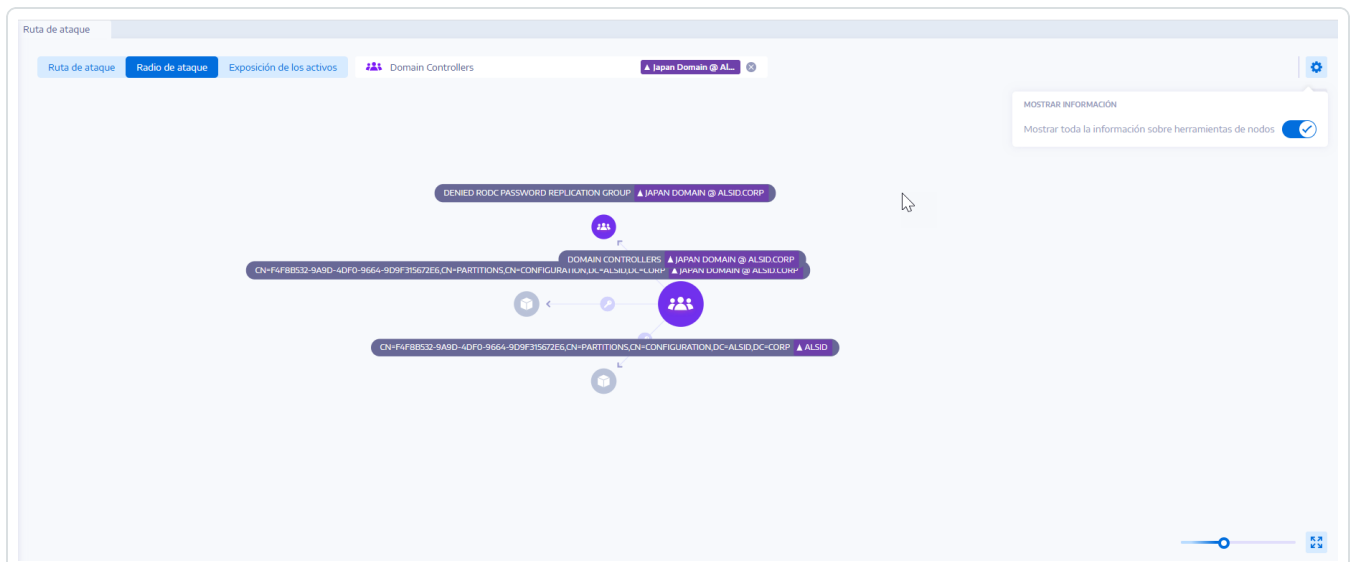
- Hacer clic en el control deslizante **Zoom** para ajustar la ampliación de los gráficos.
- Hacer clic en el conmutador **Mostrar toda la información sobre herramientas de nodos** para ver la información sobre los activos.

Para mostrar el radio de ataque:

Tenable Identity Exposure muestra una representación gráfica de la ruta de ataque potencial, donde se resaltan las conexiones entre los activos. Cada conexión representa una vulnerabilidad potencial o un error de configuración que un atacante podría aprovechar para moverse lateralmente dentro de la instancia de AD. Puede acercarse o alejar la imagen para comprender mejor los detalles de la ruta.

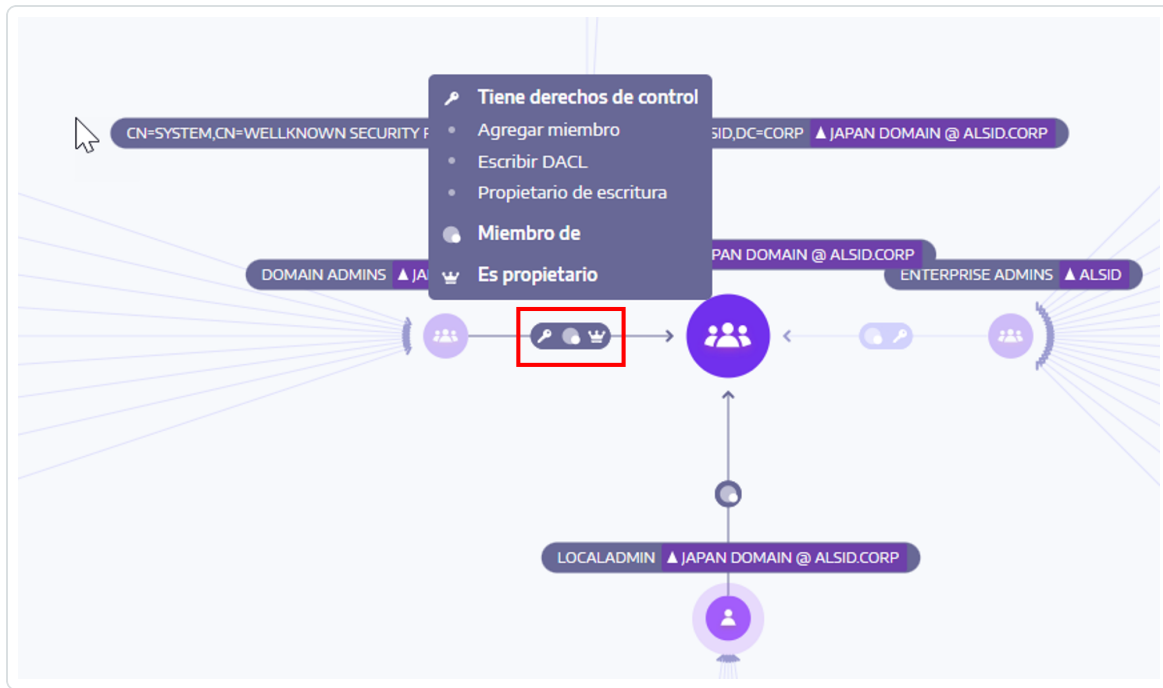
1. En Tenable Identity Exposure, haga clic en **Ruta de ataque** en el menú de la barra lateral. Aparece el panel **Ruta de ataque**.
2. En el banner, haga clic en **Radio de ataque**.
3. En el cuadro **Buscar un objeto**, escriba el nombre de un activo.
4. Haga clic en el ícono .

Tenable Identity Exposure muestra las conexiones laterales que salen de ese activo:





5. Haga clic en los íconos en las flechas entre los activos para mostrar las relaciones entre ellos.



Para visualizar la exposición de los activos:

Cada paso en la ruta de ataque se asocia a una puntuación de riesgo, que indica la gravedad de la vulnerabilidad. Esto lo ayuda a priorizar qué rutas representan la amenaza más importante y requieren atención inmediata. También puede hacer clic en puntos de conexión individuales para obtener más detalles sobre la vulnerabilidad o el error de configuración específicos relacionados.

1. En Tenable Identity Exposure, haga clic en **Ruta de ataque** en el menú de la barra lateral.

Aparece el panel **Ruta de ataque**.

2. En el banner, haga clic en **Exposición de los activos**.

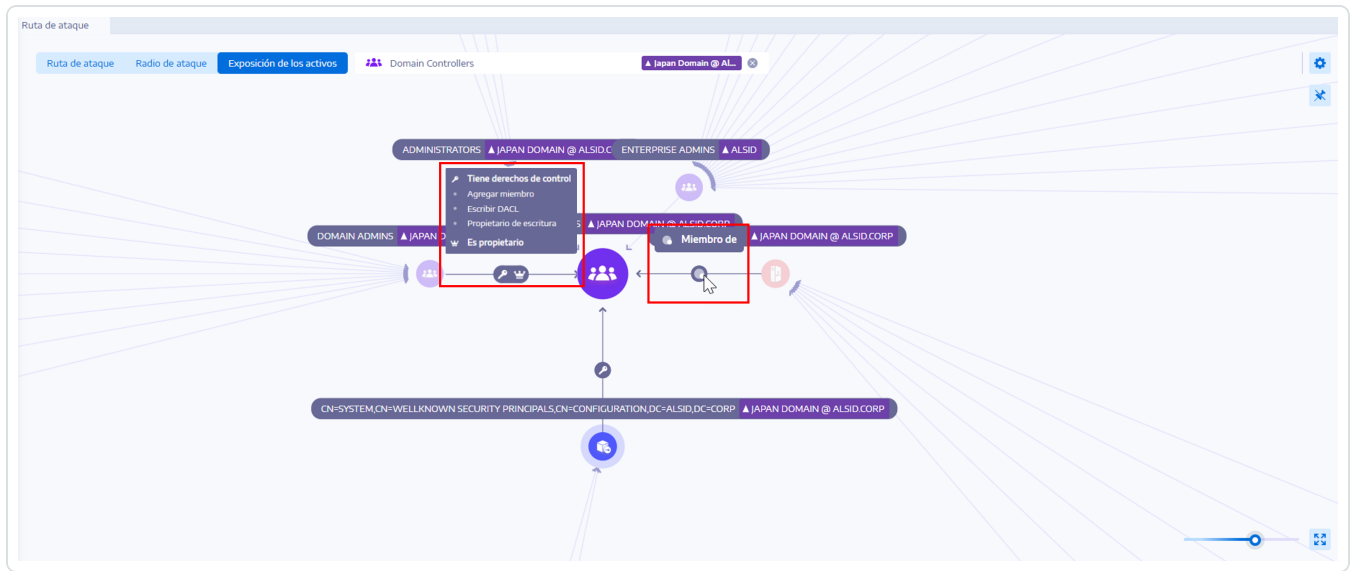
3. En el cuadro **Buscar un objeto**, escriba el nombre de un activo.

4. Haga clic en el ícono .

Tenable Identity Exposure muestra las rutas que conducen al activo y las relaciones entre los activos.




5. Haga clic en los íconos en las flechas entre los activos para mostrar las relaciones entre ellos.

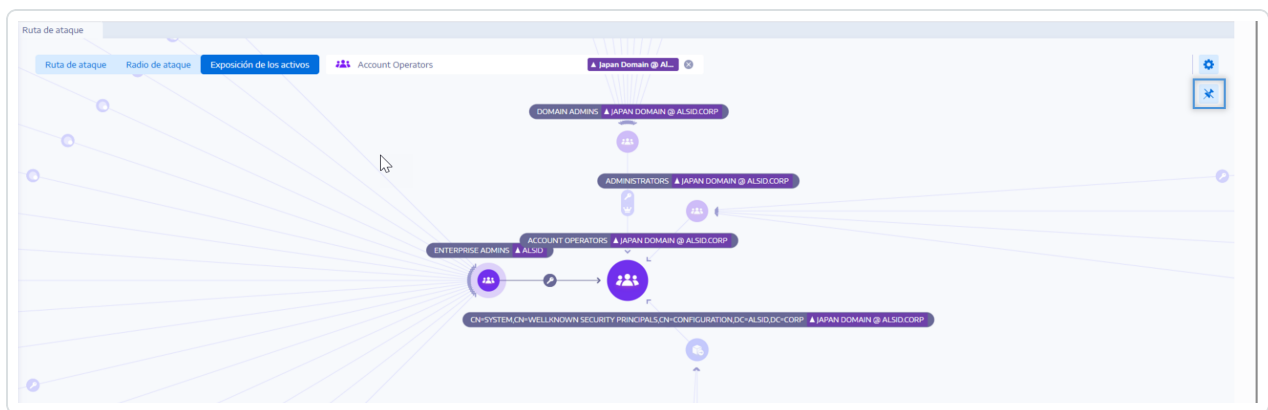


Para anclar una ruta de ataque:

1. Haga clic en un nodo que quiera resaltar en la ruta de ataque.

Tenable Identity Exposure ancla esa ruta de ataque en la pantalla.

2. Para desanclar la ruta de ataque, haga clic en el ícono  o en otro nodo en otra ruta de ataque.



Consulte también

- [Relaciones de ataque](#)
- [Identificar activos de nivel 0](#)



- [Cuentas con rutas de ataque](#)
- [Tipos de nodos de ruta de ataque](#)

Relaciones de ataque

Las relaciones de ataque son unidireccionales de un nodo de origen a un nodo de destino. Dado que las relaciones son transitivas, los atacantes pueden encadenarlas para crear una "ruta de ataque":



Tenable Identity Exposure tiene las siguientes relaciones de ataque:

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)



- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Agregar credencial de clave

Descripción

La entidad de seguridad de origen puede suplantar el destino mediante la explotación de las asignaciones de cuentas de confianza clave, también conocidas como credenciales clave o “credenciales ocultas”.

Esto es posible porque el origen tiene permiso para editar el atributo `msDS-KeyCredentialLink` del destino.

Muchas veces Windows Hello para empresas (WHfB) usa esta funcionalidad, pero los atacantes pueden explotarla incluso si no está en uso.

Explotación

Los atacantes que ponen en peligro la entidad de seguridad de origen tiene que editar el atributo `msDS-KeyCredentialLink` del equipo de destino mediante herramientas de hackeo especializadas, como Whisker o DSInternals.

El objetivo de los atacantes es agregar un nuevo certificado al atributo de este destino, para el cual tienen la clave privada. Luego pueden autenticarse como si fueran el destino con la clave privada conocida usando el protocolo PKINIT de Kerberos para obtener un TGT. Este protocolo también permite que los atacantes obtengan el hash NTLM del destino.

Corrección

Varias entidades de seguridad privilegiadas de forma nativa tienen este permiso de manera predeterminada, a saber, Operadores de cuentas, Administradores, Administradores de dominio,



Administradores de empresas, Administradores empresariales de claves, Administradores de claves y SISTEMA. Estas entidades de seguridad legítimas no requieren corrección.

Este permiso se deberá quitar de las entidades de seguridad de origen que no tengan una necesidad legítima de modificar este atributo. Busque permisos como "Escribir todas las propiedades", "Escribir msDS-AllowedToActOnBehalfOfOtherIdentity", "Control total", etc.

Consulte también

- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Agregar miembro

Descripción



La entidad de seguridad de origen puede agregarse a sí misma (derecho de escritura validado), o a cualquier otra (derecho de propiedad de escritura), como miembro del grupo de destino y beneficiarse de los derechos de acceso otorgados al grupo.

Una entidad de seguridad malintencionada que realice esta operación creará una relación de ataque "Miembro de".

Explotación

Los atacantes que ponen en peligro la entidad de seguridad de origen solo tienen que editar el atributo "miembros" del grupo de destino a través de comandos nativos de Windows (como "net group /domain"), cmdlets de PowerShell (como "Add-ADGroupMember"), herramientas de administración (como "Usuarios y equipos de Active Directory") o herramientas para hackers dedicadas (como PowerSploit).

Corrección

Si la entidad de seguridad de origen no necesita el derecho de agregar un miembro al grupo de destino, debe quitar este permiso.

Para modificar el descriptor de seguridad del grupo de destino:

1. En "Usuarios y equipos de Active Directory", haga clic con el botón derecho en **Propiedades > Seguridad**.
2. Quite permisos, como "Escribir miembros", "Escribir todas las propiedades", "Control total", "Todas las escrituras validadas", "Add/remove self as member", etc.

Nota: Un grupo puede heredar el permiso de un objeto situado más arriba en el árbol de Active Directory.

Consulte también

- [Agregar credencial de clave](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)



- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Puede actuar

Descripción

La entidad de seguridad de origen puede realizar la delegación restringida basada en recursos de Kerberos en el equipo de destino. Es decir, puede suplantar la identidad de cualquier usuario cuando se autentique con Kerberos en cualquier servicio que se ejecute en el equipo de destino.

Por lo tanto, a menudo conduce a un riesgo total en el equipo de destino.

Este ataque también se conoce como "delegación restringida basada en recursos (RBCD)", "delegación restringida basada en recursos de Kerberos (KRBCD)", "delegación restringida de Kerberos basada en recursos (RBKCD)" y "Allowed-To-Act-On-Behalf-of-Other-Identity".

Explotación

Los atacantes que ponen en peligro la entidad de seguridad de origen pueden usar herramientas para hackers dedicadas, como Rubeus, para explotar extensiones legítimas del protocolo Kerberos (S4U2self y S4U2proxy) con el fin de falsificar tickets de servicio de Kerberos y suplantar la



identidad del usuario de destino. Es probable que los atacantes elijan suplantar la identidad de un usuario privilegiado para obtener acceso privilegiado.

Una vez que los atacantes falsifican el ticket de servicio, pueden usar cualquier herramienta de administración nativa o herramienta para hackers especializada compatible con Kerberos para ejecutar comandos arbitrarios de forma remota.

Un intento de explotación exitoso debe cumplir las siguientes restricciones:

- Las entidades de seguridad de origen y de destino deben tener un atributo ServicePrincipalName. Tenable Identity Exposure no crea esta relación de ataque sin esta condición.
- La cuenta que se va a suplantar no debe estar marcada como “es importante y no se puede delegar” (ADS_UF_NOT_DELEGATED en UserAccountControl) ni ser miembro del grupo “Usuarios protegidos”, ya que Active Directory protege dichas cuentas de los ataques de delegación.

Corrección

Si la entidad de seguridad de origen no necesita el permiso para realizar la delegación restringida basada en recursos (RBCD) de Kerberos en el equipo de destino, debe quitarlo. La modificación debe hacerse en el lado de destino, a diferencia de la relación de ataque de delegación “Puede delegar”.

No es posible administrar la RBCD con las herramientas de administración gráfica existentes, como “Usuarios y equipos de Active Directory”. En su lugar, debe usar PowerShell para modificar el contenido del atributo `msDS-AllowedToActOnBehalfOfOtherIdentity`.

Use los siguientes comandos para enumerar las entidades de seguridad de origen que pueden actuar en el destino (en la sección “Acceso:”):

```
Get-ADComputer target -Properties msDS-AllowedToActOnBehalfOfOtherIdentity | Select-Object -  
ExpandProperty msDS-AllowedToActOnBehalfOfOtherIdentity | Format-List
```

Si no quiere ninguna de las entidades de seguridad que se enumeran, puede borrarlas todas con este comando:

```
Set-ADComputer target -Clear "msDS-AllowedToActOnBehalfOfOtherIdentity"
```



Si solo tiene que quitar de la lista una entidad de seguridad, por desgracia Microsoft no proporciona un comando directo. Tiene que sobrescribir el atributo con la misma lista menos el que quiera quitar. Por ejemplo, si se permiten "sourceA", "sourceB" y "sourceC" y quiere solo "sourceB", ejecute:

```
Set-ADComputer target -PrincipalsAllowedToDelegateToAccount (Get-ADUser sourceA),(Get-ADUser sourceC)
```

Por último, como recomendación general, para limitar la exposición de las cuentas privilegiadas confidenciales a dichos ataques de delegación, Tenable Identity Exposure recomienda que se marquen como "es importante y no se puede delegar" (ADS_UF_NOT_DELEGATED) o se agreguen al grupo "Usuarios protegidos", después de una verificación cuidadosa de los efectos operativos asociados.

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)



- [Escribir DACL](#)
- [Escribir propietario](#)

Puede delegar

Descripción

La entidad de seguridad de origen puede realizar la delegación restringida de Kerberos (KCD) con transición de protocolos en el equipo de destino. Es decir, puede suplantar la identidad de cualquier usuario cuando se autentique con Kerberos en cualquier servicio que se ejecute en el equipo de destino.

Por lo tanto, a menudo conduce a un riesgo total en el equipo de destino.

Explotación

Los atacantes que ponen en peligro la entidad de seguridad de origen pueden usar herramientas para hackers dedicadas, como Rubeus, para explotar extensiones legítimas del protocolo Kerberos (S4U2self y S4U2proxy) con el fin de falsificar tickets de servicio de Kerberos y suplantar la identidad del usuario de destino. Es probable que los atacantes elijan suplantar la identidad de un usuario privilegiado para obtener acceso privilegiado.

Una vez que los atacantes falsifican el ticket de servicio, pueden usar cualquier herramienta de administración nativa o herramienta para hackers especializada compatible con Kerberos para ejecutar comandos arbitrarios de forma remota.

Un intento de explotación exitoso debe cumplir las siguientes restricciones:

- La entidad de seguridad de origen debe estar habilitada para la transición de protocolos (ADS_UF_TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION en UserAccountControl o "Usar cualquier protocolo de autenticación" en la GUI de delegación). Más precisamente, el ataque podría funcionar sin transición de protocolos ("Usar solamente Kerberos" en la GUI de delegación), pero los atacantes primero deben forzar una autenticación de Kerberos del usuario objetivo en la entidad de seguridad de origen, lo que hace que el ataque sea más difícil. Por lo tanto, en este caso Tenable Identity Exposure no crea una relación de ataque.



- Las entidades de seguridad de origen y de destino deben tener un atributo ServicePrincipalName. Tenable Identity Exposure no crea esta relación de ataque sin esta condición.
- La cuenta que se va a suplantar no debe estar marcada como “es importante y no se puede delegar” (ADS_UF_NOT_DELEGATED en UserAccountControl) ni ser miembro del grupo “Usuarios protegidos”, ya que Active Directory protege dichas cuentas de los ataques de delegación.

Por el contrario, el equipo de destino donde se permite la delegación está designado por un nombre de entidad de servicio (SPN) y, por lo tanto, contiene un servicio específico, como SMB con “cifs/host.example.net”, HTTP con “http/host.example.net”, etc. Sin embargo, los atacantes pueden apuntar a cualquier otro SPN y servicio que se ejecute bajo la misma cuenta de destino mediante un “ataque de sustitución de sname”. Por lo tanto, esto no constituye una limitación.

Corrección

Si la entidad de seguridad de origen no necesita el permiso para realizar la delegación restringida de Kerberos (KCD) en el equipo de destino, debe quitarlo. La modificación debe hacerse en el lado de origen, a diferencia de una relación de ataque de delegación “Puede actuar”.

Para quitar la entidad de seguridad de origen:

1. En la GUI de administración de “Usuarios y equipos de Active Directory”, vaya a la pestaña **Propiedades > Delegación** del objeto de origen.
2. Quite el nombre de entidad de servicio correspondiente al destino.
3. Si no quiere ninguna delegación de este origen, quite todos los SPN y seleccione “No confiar en este equipo para la delegación”.

Como alternativa, puede usar PowerShell para modificar el contenido del atributo “msDS-AllowedToDelegateTo” del origen.

- Por ejemplo, en PowerShell, ejecute este comando para reemplazar todos los valores:

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Replace @{ "msDS-AllowedToDelegateTo" = @("cifs/desiredTarget.example.net") }
```



- Si no quiere ninguna delegación de este origen, ejecute el siguiente comando para borrar el atributo:

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Clear "msDS-AllowedToDelegateTo"
```

También es posible deshabilitar la transición de protocolos para reducir el riesgo sin cerrar por completo esta ruta de ataque. Esto requiere que todas las entidades de seguridad se conecten al origen usando solamente Kerberos en lugar de NTLM.

Para deshabilitar la transición de protocolos:

1. En la GUI de administración de “Usuarios y equipos de Active Directory”, vaya a la pestaña **Propiedades > Delegación** del objeto de origen.
2. Seleccione “Usar solamente Kerberos” en lugar de “Usar cualquier protocolo de autenticación”.

Como alternativa, puede ejecutar el siguiente comando en PowerShell para deshabilitar la transición de protocolos:

```
Set-ADAccountControl -Identity "CN=Source,OU=corp,DC=example,DC=net" -TrustedToAuthForDelegation $false
```

Por último, como recomendación general, para limitar la exposición de las cuentas privilegiadas confidenciales a dichos ataques de delegación, Tenable Identity Exposure recomienda que se marquen como “Es importante y no se puede delegar” (ADS_UF_NOT_DELEGATED) o se agreguen al grupo “Usuarios protegidos”, después de una verificación cuidadosa de los efectos operativos asociados.

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Pertenece a GPO](#)
- [DCSync](#)



- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Pertenece a GPO

Descripción

El archivo o carpeta de GPO de origen en el recurso compartido de SYSVOL pertenece al GPC (GPO) de destino, lo que significa que define las configuraciones o los programas o scripts que aplica el GPO.

Explotación

Esta no es una relación de ataque que un atacante usaría de forma aislada. Sin embargo, a modo de ejemplo, puede mostrar rutas de ataque completas donde los atacantes que tienen control de un archivo o carpeta de GPO perteneciente a un GPO pueden forzar configuraciones arbitrarias o ejecutar scripts en los usuarios o equipos al final de la ruta de ataque.

Corrección

Esta relación muestra cómo los archivos y carpetas de GPO que se encuentran en SYSVOL se relacionan con el objeto del GPC (GPO) correspondiente. Esto es normal y se diseñó así.

Por lo tanto, no hay necesidad de ninguna corrección.



Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

DCSync

Descripción

DCSync es una funcionalidad legítima de Active Directory que los controladores de dominio solo usan para replicar cambios, pero las entidades de seguridad ilegítimas también pueden usarla.

La entidad de seguridad de origen puede solicitar secretos confidenciales (hashes de contraseñas, claves de Kerberos, etc.) del dominio de destino mediante la funcionalidad DCSync, lo que, en definitiva, pone en total peligro al dominio.



Para obtener secretos, se requieren dos permisos de seguridad: “Replicar cambios de directorio” (DS-Replication-Get-Changes) y “Replicar todos los cambios de directorio” (DS-Replication-Get-Changes-All). La relación solo tiene lugar si otorga ambos permisos al origen, ya sea directamente o a través de la membresía a grupos anidados.

Explotación

Los atacantes que ponen en peligro la entidad de seguridad de origen pueden obtener secretos a través de herramientas para hackers dedicadas, como *mimikatz* o *impacket*.

- **Golden Ticket:** resultados de la obtención del hash de la contraseña de la cuenta “KRBTGT”, lo que permite falsificar un TGT de Kerberos y suplantar la identidad de cualquier usuario en cualquier equipo o servicio. En particular, esto otorga privilegios administrativos sobre cualquier equipo del dominio.
- **Silver Ticket:** resultado de la obtención del hash de la contraseña de una cuenta de equipo o de servicio, lo que permite falsificar un ticket de servicio de Kerberos y permite suplantar la identidad de cualquier usuario en el equipo o servicio dados.

Corrección

Las entidades de seguridad legítimas permitidas de manera predeterminada que pueden aprovechar DCSync son:

- Administradores
- Administradores de dominio
- Administradores de empresas
- SISTEMA

Además, la configuración de Microsoft Entra ID Connect permite que su cuenta de servicio de sincronización de hashes de contraseña (MSOL_...) aproveche DCSync.

Por último, es posible detectar cuentas de servicio para ciertas herramientas de seguridad, en particular soluciones de auditoría de contraseñas. Compruebe su legitimidad con los responsables.

Este permiso se deberá quitar de las entidades de seguridad de origen que no tengan una necesidad legítima de usar DCSync.

Para modificar el descriptor de seguridad del dominio de destino:



1. En "Usuarios y equipos de Active Directory", haga clic con el botón derecho en el nombre del dominio y seleccione "Propiedades" > "Seguridad".
2. Elimine los permisos "Replicar cambios de directorio" y "Replicar todos los cambios de directorio" para las entidades de seguridad ilegítimas.

Nota: Las relaciones de DCSync pueden ocurrir a través de permisos de pertenencia a grupos anidados. Por lo tanto, en función de la situación exacta, debe quitar los grupos en sí o solo algunos de sus miembros.

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Concesión dada para actuar



Descripción

La entidad de seguridad de origen puede otorgarse a sí misma o a otra una relación [Puede actuar](#) con el equipo de destino. A menudo, esto lleva a poner en total peligro el equipo de destino a través de un ataque de delegación de RBCD de Kerberos.

Esto es posible porque el origen tiene permiso para editar el atributo "msDS-AllowedToActOnBehalfOfOtherIdentity" del destino.

Una entidad de seguridad malintencionada que realice esta operación puede crear una relación de ataque "Puede actuar".

Explotación

Los atacantes que pongan en peligro la entidad de seguridad de origen deben editar el atributo `msDS-AllowedToActOnBehalfOfOtherIdentity` del equipo de destino mediante PowerShell (por ejemplo, "Set-ADComputer <target> -PrincipalsAllowedToDelegateToAccount...").

Corrección

Varias entidades de seguridad privilegiadas de forma nativa tienen este permiso de manera predeterminada, a saber, Operadores de cuentas, Administradores, Administradores de dominio, Administradores de empresas y SISTEMA. Estas entidades de seguridad son legítimas y no requieren corrección.

La RBCD de Kerberos se diseñó para que los administradores de un equipo puedan otorgar los derechos para realizar delegaciones en el equipo a cualquier usuario que lo necesite. Esto difiere de otros modos de delegación de Kerberos que requieren el permiso de nivel Administradores de dominio. Esto permite que administradores de nivel inferior gestionen estas opciones de seguridad por sí mismos, que es un principio también conocido como "delegación". En este caso, la relación es legítima.

Sin embargo, si la entidad de seguridad de origen no es un administrador legítimo del equipo de destino, la relación no es legítima y debe quitarse este permiso.

Para modificar el descriptor de seguridad del equipo de destino:



1. En "Usuarios y equipos de Active Directory", haga clic con el botón derecho en **Propiedades > Seguridad**.
2. Quite el permiso dado a la entidad de seguridad de origen. Busque permisos como "Escribir msDS-AllowedToActOnBehalfOfOtherIdentity", "Escribir todas las propiedades", "Write account restrictions", "Control total", etc.

Nota: La entidad de seguridad de origen puede heredar el permiso de un objeto situado más arriba en el árbol de Active Directory.

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)



Tiene historial de SID

Descripción

La entidad de seguridad de origen tiene el identificador de seguridad de la entidad de seguridad de destino en su atributo SIDHistory, lo que hace que el origen tenga los mismos derechos que el destino.

El historial de SID es un mecanismo legítimo que se usa al migrar entidades de seguridad entre dominios para mantener funcionales todas las autorizaciones que hacen referencia a su identificador de seguridad anterior.

Sin embargo, este también es un mecanismo de persistencia que usan los atacantes, ya que permite que una cuenta con una puerta trasera discreta tenga los mismos derechos que el destino deseado, como una cuenta de administrador.

Explotación

Los atacantes que ponen en peligro la entidad de seguridad de origen pueden autenticarse directamente como la entidad de seguridad de destino, ya que el identificador de seguridad del destino se agrega de forma transparente al token que generan los mecanismos de autenticación de Active Directory (NTLM y Kerberos).

Corrección

Si las entidades de seguridad de origen y destino están relacionadas con una migración de dominio aprobada, puede considerar que la relación es legítima y no hacer nada. Esta relación se mantiene visible como recordatorio de una posible ruta de ataque.

Si el dominio de origen se eliminó después de la migración o no está configurado en Tenable Identity Exposure, la entidad de seguridad de destino se marca como sin resolver. Dado que el riesgo reside en el destino y este no existe, no hay riesgo y, por lo tanto, no se requiere ninguna corrección.

Por el contrario, es muy probable que las relaciones del historial de SID con usuarios o grupos con privilegios de forma nativos sean malintencionadas, ya que Active Directory impide su creación. Es decir, probablemente se crearon usando técnicas de hackers, como un ataque "DCShadow". También puede encontrar estos casos en el IoE relacionado con "Historial de SID".



Si es así, Tenable Identity Exposure recomienda un examen forense de todo el bosque de Active Directory. La razón es que los atacantes deben haber obtenido privilegios elevados (administrador de dominio o equivalente) para editar de forma malintencionada el historial de SID del origen. El examen forense lo ayuda a analizar el ataque con la guía de corrección correspondiente e identifica posibles puertas traseras para eliminar.

Por último, Microsoft recomienda modificar todos los derechos de acceso en todos los servicios (recursos compartidos de SMB, Exchange, etc.) para usar los nuevos identificadores de seguridad y eliminar los valores de SIDHistory innecesarios una vez que se complete esta migración. Esta es una práctica recomendada de mantenimiento, aunque identificar exhaustivamente y corregir todas las ACL es muy difícil.

Un usuario que tenga derecho a editar el atributo SIDHistory en el objeto de origen en sí puede quitar los valores de SIDHistory. Al contrario de la creación, esta operación no requiere derechos de administrador de dominio.

Para hacer esto, solo puede usar PowerShell, dado que las herramientas gráficas, como Usuarios y equipos de Active Directory, fallarán. Ejemplo:

```
Set-ADUser -Identity <user> -Remove @{sidhistory="S-1-..."}
```

Precaución: Si bien eliminar un valor de SIDHistory es sencillo, revertir esta operación es muy complicado. Esto se debe a que tiene que volver a crear el valor de SIDHistory, lo que requiere la presencia del otro dominio, que tal vez haya quedado fuera de servicio. Por este motivo, Microsoft también recomienda preparar instantáneas o copias de seguridad.

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)



- [Concesión dada para actuar](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Toma de control implícita

Descripción

El origen es una entidad de seguridad de nivel 0. El nivel 0 es el conjunto de objetos de Active Directory que tienen los privilegios más altos en el dominio, como los miembros del grupo Administradores de dominio o Controladores de dominio. Todos los activos de nivel 0 pueden poner en peligro implícitamente cualquier otro objeto del dominio, incluso si no existe otra relación explícita.

Esta relación hace posible modelar derechos implícitos integrados en Active Directory. Estos derechos se diseñaron así y están documentados y, por lo tanto, los atacantes los conocen. Sin embargo, Tenable Identity Exposure no puede recopilar estos derechos por medios estándar. Además, esta relación simplifica los gráficos de rutas de ataque, porque, tan pronto como los atacantes ponen en peligro un nodo de nivel 0, pueden atacar cualquier otro objeto directamente sin tener que pasar por otras relaciones explícitas.

En resumen, se considera que todos los activos de nivel 0 de origen tienen relaciones de "toma de control implícita" con cualquier nodo de destino en el gráfico.

Explotación



El método de explotación exacto depende del tipo de activo de nivel 0 de origen que sea el objetivo, pero se trata de técnicas bien documentadas que los atacantes dominan por completo.

Corrección

Esta relación se diseñó así y no se puede corregir. Es casi imposible evitar que un atacante que alcance un activo de nivel 0 siga atacando.

Los esfuerzos de corrección deben centrarse en las relaciones ascendentes en las rutas de ataque.

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Heredar GPO



Descripción

Un contenedor vinculable de origen, como una unidad organizativa (OU) o un dominio (pero no sitios), contiene la OU de destino, el usuario, el dispositivo, el controlador de dominio o el controlador de dominio de solo lectura (RODC) en el árbol de LDAP. Esto se debe a que los objetos secundarios del contenedor vinculable heredan el GPO donde está vinculado (consulte las relaciones "GPO vinculado").

Tenable Identity Exposure tiene en cuenta siempre que una OU bloquea la herencia.

Explotación

Los atacantes no tienen nada que hacer para explotar esta relación siempre que logren poner en peligro el GPO en un punto anterior de la ruta de ataque. Por diseño, la relación se aplica a los contenedores vinculables y a los objetos debajo de ellos, como lo muestran las relaciones "Heredar GPO".

Corrección

En la mayoría de los casos, es normal y legítimo que los GPO se apliquen a los contenedores secundarios vinculables desde sus contenedores principales. Sin embargo, esta vinculación expone rutas de ataque adicionales.

Por lo tanto, para reducir los riesgos, debe vincular los GPO al nivel más bajo en la jerarquía de unidades organizativas, siempre que sea posible.

Además, los GPO requieren protección frente a modificaciones no autorizadas por parte de atacantes con el fin de no exponerlos a otras relaciones de ataque.

Por último, las OU pueden deshabilitar la herencia de GPO de niveles superiores a través de la opción "bloquear herencia". Sin embargo, utilice esta opción solo como último recurso, ya que bloquea todos los GPO, incluidos los GPO de endurecimiento de la seguridad potenciales definidos en el nivel de dominio más alto. Además, dificulta el razonamiento sobre los GPO aplicados.

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)



- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

GPO vinculado

Descripción

El GPO de origen está vinculado al contenedor vinculable de destino, como un dominio o una unidad organizativa (OU). Es decir, el GPO de origen puede asignar configuraciones y ejecutar programas en los dispositivos y usuarios contenidos en el destino. El GPO de origen también se aplica a los objetos en contenedores debajo de él a través de relaciones "Heredar GPO".

En definitiva, el GPO puede poner en peligro los dispositivos y usuarios a los que se aplica.

Explotación

Los atacantes primero deben poner en peligro el GPO de origen a través de otra relación de ataque.



Desde allí, emplean varias técnicas para realizar acciones malintencionadas sobre los dispositivos y usuarios contenidos en el destino y aquellos debajo de él. Entre otros ejemplos:

- Aprovechase de las “tareas programadas inmediatas” legítimas para ejecutar scripts arbitrarios en los dispositivos.
- Agregar un nuevo usuario local con derechos administrativos en todos los dispositivos.
- Instalar un programa MSI.
- Deshabilitar el firewall o antivirus.
- Conceder derechos adicionales.
- Otras acciones.

Para modificar un GPO, los atacantes pueden editar manualmente su contenido mediante herramientas de administración, como “Administración de directivas de grupo”, o herramientas para hackers dedicadas, como PowerSploit.

Corrección

En la mayoría de los casos, vincular un GPO a un contenedor vinculable es algo normal y legítimo. Sin embargo, este vínculo aumenta la superficie de ataque donde tiene lugar, así como en los contenedores debajo de él.

Por lo tanto, para reducir los riesgos, debe vincular los GPO al nivel más bajo en la jerarquía de unidades organizativas, siempre que sea posible.

Además, los GPO requieren protección frente a modificaciones no autorizadas por parte de atacantes con el fin de no exponerlos a otras relaciones de ataque.

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)



- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Miembro de

Descripción

La entidad de seguridad de origen es miembro del grupo de destino. Por lo tanto, se beneficia de todos los derechos de acceso que posee el grupo, como acceder a recursos compartidos de archivos, asumir roles en aplicaciones empresariales, etc.

Explotación

Los atacantes no tienen que hacer nada para explotar esta relación de ataque. Solo tienen que autenticarse como entidad de seguridad de origen para obtener el grupo de destino en su token de seguridad local o remoto, o en su ticket de Kerberos.

Corrección

Si la entidad de seguridad de origen es miembro ilegítimo del grupo de destino, debe eliminarlo.

Puede usar cualquier herramienta de administración de Active Directory estándar, como "Usuarios y equipos de Active Directory", o cmdlet de PowerShell, como Remove-ADGroupMember.



Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Es propietario

Descripción

La entidad de seguridad de origen es el propietario declarado del objeto de destino porque probablemente creó el objeto de destino. Los propietarios tienen derechos implícitos (“Control de lectura” y “Escritura DACL”) que les permiten obtener derechos adicionales, para sí mismos o para otra persona, y, en última instancia, poner en peligro el objeto de destino.

Explotación



Los atacantes que ponen en peligro la entidad de seguridad de origen solo tienen que editar el descriptor de seguridad del objeto de destino a través de comandos nativos de Windows (como "dsacls"), cmdlets de PowerShell (como "Set-ACL"), herramientas de administración (como "Usuarios y equipos de Active Directory") o herramientas para hackers dedicadas (como PowerSploit).

Cuando se crea un objeto, existe el riesgo de escalamiento de privilegios si un usuario con pocos privilegios lo crea y, por lo tanto, es su propietario (por ejemplo, un técnico de soporte estándar) y, luego, se elevan los privilegios de ese objeto (por ejemplo, a administrador). El propietario original permanece y ahora puede poner en peligro el objeto recientemente privilegiado para aprovechar sus privilegios.

Corrección

Si la entidad de seguridad de origen no es miembro legítimo del objeto de destino, debe cambiarlo.

Para cambiar el propietario del objeto de destino:

1. En "Usuarios y equipos de Active Directory", haga clic con el botón derecho en **Propiedades > Seguridad > Opciones avanzadas**.
2. En la línea **Propietario** del principio, haga clic en **Cambiar**.

Los propietarios de objetos de destino seguros usados de manera predeterminada para la mayoría de los objetos confidenciales de Active Directory son:

- Objetos en la partición del dominio: "Administradores" o "Administradores de dominio"
- Objetos en la partición de configuración: "Administradores de empresas"
- Objetos en la partición de esquema: "Administradores de esquema"

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)



- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Restablecer la contraseña

Descripción

La entidad de seguridad de origen puede restablecer la contraseña del destino, lo que le permite autenticarse como el destino usando la nueva contraseña atribuida y aprovecharse de los privilegios del destino.

Restablecer una contraseña no es lo mismo que cambiar una contraseña, algo que puede hacer cualquiera que conozca la contraseña actual. En general, un cambio de contraseña se produce cuando una contraseña vence.

Explotación

Los atacantes que ponen en peligro la entidad de seguridad de origen pueden restablecer la contraseña del destino a través de comandos nativos de Windows (como "net user /domain"), cmdlets de PowerShell (como "Set-ADAccountPassword - Reset"), herramientas de administración (como "Usuarios y equipos de Active Directory") o herramientas para hackers dedicadas (como PowerSploit).



Los atacantes luego solo tienen que autenticarse en Active Directory o en el recurso de destino usando métodos de autenticación legítimos con la nueva contraseña elegida para suplantar por completo la identidad del destino.

No obstante, los atacantes en general no conocen la contraseña anterior para revertirla después del ataque. Por lo tanto, a menudo la persona legítima detrás del destino puede ver el ataque, que incluso puede provocar una denegación de servicio, en especial si se trata de cuentas de servicio.

Corrección

Los administradores de TI y el personal de soporte técnico pueden de forma legítima restablecer contraseñas. No obstante, es necesario establecer las delegaciones adecuadas para que puedan realizar esta acción solo dentro de su perímetro permitido.

Además, de acuerdo con el modelo de niveles, debe asegurarse de que el personal de un nivel inferior, como el servicio de soporte para usuarios normales, no pueda restablecer la contraseña de una cuenta de nivel superior, como la de un administrador de dominio, porque esta es una oportunidad para el escalamiento de privilegios.

Para modificar el descriptor de seguridad del destino y quitar permisos ilegítimos:

1. En "Usuarios y equipos de Active Directory", haga clic con el botón derecho en "Propiedades" > "Seguridad".
2. Quite el permiso "Restablecer contraseña" de la entidad de seguridad de origen.

Nota: No confunda este permiso con "Cambiar contraseña".

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)



- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Gestión de RODC

Descripción

La entidad de seguridad de origen se encuentra en el atributo "ManagedBy" del controlador de dominio de solo lectura (RODC) de destino. Es decir, el origen tiene derechos administrativos sobre el RODC de destino.

Nota: Otros tipos de objetos de Active Directory usan el mismo atributo "ManagedBy" solo con fines informativos y no otorgan ningún derecho administrativo al administrador declarado. Por lo tanto, esta relación solo existe para los nodos de destino del tipo RODC.

Los RODC son menos confidenciales que los controladores de dominio que permiten escritura más comunes, pero siguen siendo un objetivo de alto valor para los atacantes, ya que pueden robar credenciales de los RODC para permitirles acceder a otros sistemas. Esto depende del nivel de endurecimiento de la configuración del RODC; por ejemplo, la cantidad de objetos con secretos que puede sincronizar.

Explotación

El método de explotación es idéntico al de la relación "AdminTo".



Los atacantes que ponen en peligro la entidad de seguridad de origen pueden usar su identidad para conectarse de forma remota y ejecutar comandos en el RODC de destino con derechos administrativos. Pueden explotar protocolos nativos disponibles, como bloque de mensajes del servidor (SMB), con recursos compartidos administrativos, Protocolo de escritorio remoto (RDP), Instrumental de administración de Windows (WMI), llamada a procedimiento remoto (RPC), Administración remota de Windows (WinRM), etc.

Los atacantes pueden usar herramientas de administración remota nativas, como PsExec, servicios, tareas programadas, Invoke-Command, etc., o herramientas para hackers especializadas, como wmiexec, smbexec, Invoke-DCOM, SharpRDP, etc.

El objetivo final del ataque puede ser poner en peligro el RODC de destino o usar herramientas de volcado de credenciales, como mimikatz, para obtener más credenciales y secretos para acceder a otras máquinas.

Corrección

Si la entidad de seguridad de origen no es un administrador legítimo del controlador de dominio de solo lectura (RODC) de destino, deberá reemplazarlo por un administrador adecuado.

Tenga en cuenta que, en general, los administradores de dominio no administran los RODC, de ahí la opción dedicada “administrado por”. Esto se debe a que los RODC tienen un nivel de confianza más bajo y los administradores de dominio con altos privilegios no deberían exponer sus credenciales al autenticarse en ellos.

Por lo tanto, debe seleccionar un administrador de “nivel medio” adecuado para los RODC de acuerdo con las reglas de RODC de Active Directory; por ejemplo, el administrador de TI de la sucursal local de una organización donde se encuentran.

Para cambiar el atributo “ManagedBy”:

1. En “Usuarios y equipos de Active Directory”, seleccione la pestaña “RODC” > **Propiedades** > **ManagedBy**.
2. Haga clic en **Cambiar**.

También puede ejecutar el siguiente comando en PowerShell:

```
Set-ADComputer <rodc> -ManagedBy (Get-ADUser <rodc_admin>)
```



Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Escribir DACL](#)
- [Escribir propietario](#)

Escribir DACL

Descripción

La entidad de seguridad de origen tiene el permiso para cambiar los permisos del objeto de destino en la lista de control de acceso discrecional (DACL). Esto permite que el origen obtenga para sí mismo, o le dé a alguien más, derechos adicionales y, en última instancia, ponga en peligro el objeto de destino.

Explotación



Los atacantes que ponen en peligro la entidad de seguridad de origen solo tienen que editar el descriptor de seguridad del objeto de destino a través de comandos nativos de Windows (como "dsacls"), cmdlets de PowerShell (como "Set-ACL"), herramientas de administración (como "Usuarios y equipos de Active Directory") o herramientas para hackers dedicadas (como PowerSploit).

Corrección

Si la entidad de seguridad de origen no tiene permiso legítimo para cambiar los permisos del objeto de destino, deberá quitar este permiso.

Para modificar el descriptor de seguridad del objeto de destino:

1. En "Usuarios y equipos de Active Directory", haga clic con el botón derecho en el objeto y haga clic en **Propiedades > Seguridad > Opciones avanzadas**.
2. Quite el permiso "Modificar permisos" de la entidad de seguridad de origen.

Nota: Un objeto puede heredar el permiso de un objeto situado más arriba en el árbol de Active Directory.

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)



- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir propietario](#)

Escribir propietario

Descripción

La entidad de seguridad de origen tiene permiso para cambiar el propietario del objeto de destino, lo que incluye asignarse a sí mismo como propietario. Los propietarios tienen derechos implícitos, "Control de lectura" y "Escribir DACL", que les permiten obtener derechos adicionales, para sí mismos o para otra persona, y, en última instancia, poner en peligro el objeto de destino.

Para obtener más información, consulte la relación [Es propietario](#).

Explotación

Los atacantes que ponen en peligro la entidad de seguridad de origen pueden asignarse a sí mismos como propietario del destino a través de comandos nativos de Windows (como "dscls /takeownership"), cmdlets de PowerShell (como "Set-ACL"), herramientas de administración (como "Usuarios y equipos de Active Directory") o herramientas para hackers dedicadas (como PowerSploit).

Luego pueden editar el descriptor de seguridad del objeto de destino con métodos similares.

Corrección

Si la entidad de seguridad de origen no tiene permiso legítimo para cambiar el propietario del objeto de destino, deberá quitar este permiso.

Para modificar el descriptor de seguridad del objeto de destino:



1. En "Usuarios y equipos de Active Directory", haga clic con el botón derecho en el objeto y seleccione **Propiedades > Seguridad > Opciones avanzadas**.
2. Quite el permiso "Modificar propietario" de la entidad de seguridad de origen.

Nota: Un objeto puede heredar el permiso de un objeto situado más arriba en el árbol de Active Directory.

Consulte también

- [Agregar credencial de clave](#)
- [Agregar miembro](#)
- [Puede actuar](#)
- [Puede delegar](#)
- [Pertenece a GPO](#)
- [DCSync](#)
- [Concesión dada para actuar](#)
- [Tiene historial de SID](#)
- [Toma de control implícita](#)
- [Heredar GPO](#)
- [GPO vinculado](#)
- [Miembro de](#)
- [Es propietario](#)
- [Restablecer la contraseña](#)
- [Gestión de RODC](#)
- [Escribir DACL](#)


Identificar activos de nivel 0

Los activos de nivel 0 incluyen cuentas, grupos y otros activos que tienen un control administrativo directo o indirecto de los bosques y dominios de Active Directory.



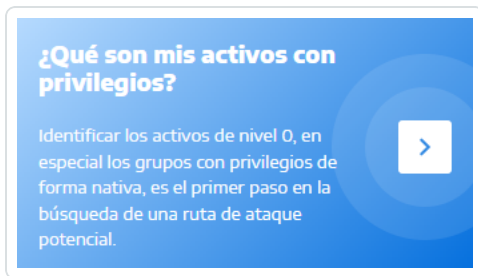
Tenable Identity Exposure enumera los activos y cuentas de nivel 0 con posibles rutas de ataque que conducen a ese activo.

Para enumerar activos de nivel 0:

1. En Tenable Identity Exposure, haga clic en el ícono de ruta de ataque  en la barra de navegación de la izquierda.

Se abre el panel **Ruta de ataque**.

2. Haga clic en el mosaico **¿Qué son mis activos con privilegios?**



Tenable Identity Exposure muestra una lista de activos de nivel 0 en su instancia de AD.

La interfaz muestra una lista de activos de nivel 0 con las siguientes columnas: NOMBRE, DOMINIO, CUENTAS CON RUTA DE ATAQUE y EXPOSICIÓN. Hay un botón de búsqueda y un botón de acciones para cada fila.

NOMBRE	DOMINIO	CUENTAS CON RUTA DE ATAQUE	EXPOSICIÓN
Account Operators	Japan Domain @ Alsid.corp	101	194.23%
Administrators	Japan Domain @ Alsid.corp	101	194.23%
Backup Operators	Japan Domain @ Alsid.corp	102	196.15%
CN=Enterprise Domain Controllers,CN=WellKnown Security Principals,CN=Configura...	Japan Domain @ Alsid.corp	101	194.23%
CN=System,CN=WellKnown Security Principals,CN=Configuration,DC=alsid,DC=corp	Japan Domain @ Alsid.corp	101	194.23%
Cert Publishers	Japan Domain @ Alsid.corp	101	194.23%

Cada línea proporciona el **nombre del activo**, su **dominio** y la siguiente información:

- **Cuentas con ruta de ataque:** la cantidad de activos que tienen una ruta de ataque que conduce al activo de nivel 0.
- **Exposición:** las cuentas que tienen una ruta de ataque que conduce al activo de nivel 0 como porcentaje del número total de cuentas en el dominio.

Para filtrar los activos de un dominio en particular:



1. Haga clic en el botón **n/n**.

Se abre el panel **Bosques y dominios**. Puede seguir cualquiera de los siguientes procedimientos:

- En el cuadro **Buscar**, escriba el nombre de un bosque o dominio.
- Seleccione la casilla **Expandir todo** y seleccione el bosque o dominio que quiera.

2. Haga clic en **Filtrar selección**.

Tenable Identity Exposure actualiza la lista de activos.

Para enumerar las cuentas con rutas de ataque que conducen al activo de nivel 0:

- Al final de la línea del nombre del activo de nivel 0, haga clic en el ícono .

Tenable Identity Exposure muestra una lista de las cuentas con rutas de ataque que conducen al activo de nivel 0.

Para ver la exposición de activos del activo de nivel 0:

- Al final de la línea del nombre del activo de nivel 0, haga clic en el ícono .

Tenable Identity Exposure abre la página "Exposición de activos" para ese activo de nivel 0.


Para obtener más información, consulte [Relaciones de ataque](#).

Cuentas con rutas de ataque

Tenable Identity Exposure muestra cuentas con rutas de ataque que llevan a activos de nivel 0 para brindarle una vista exhaustiva de una posible amenaza de seguridad, dado que las cuentas de usuario y de equipo pueden volverse privilegiadas a través de varias relaciones de ataque.

Para obtener más información, consulte [Identificar activos de nivel 0](#).

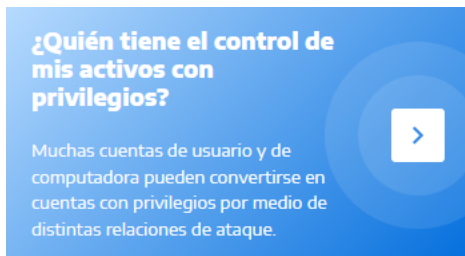
Para mostrar activos con rutas de ataque:

1. En Tenable Identity Exposure, haga clic en el ícono de ruta de ataque  en la barra de navegación de la izquierda.

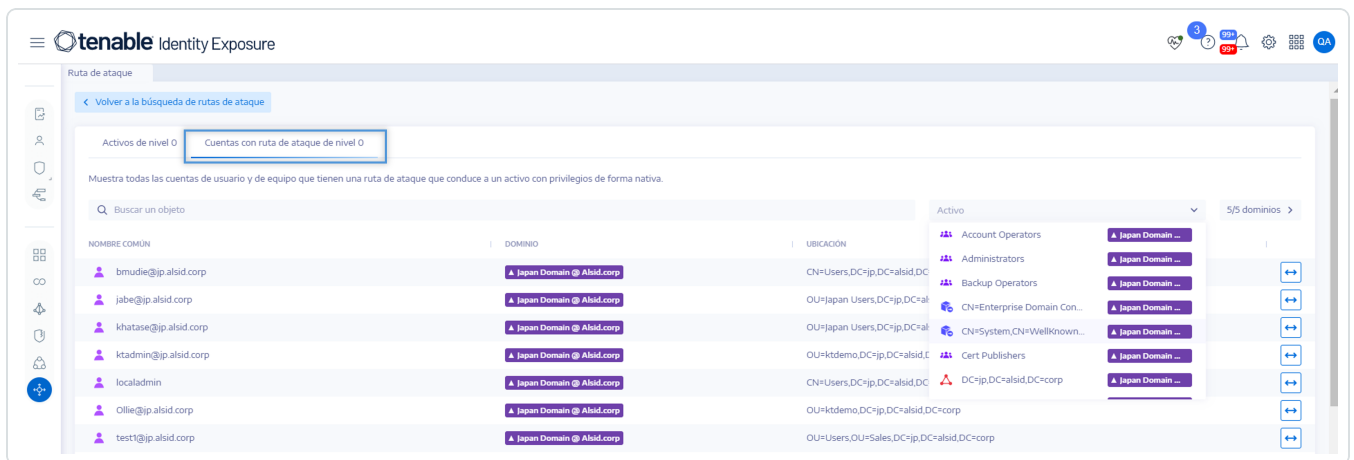
Se abre el panel **Ruta de ataque**.



2. Haga clic en el mosaico **¿Quién tiene el control de mis activos con privilegios?**



Tenable Identity Exposure muestra todas las cuentas de usuario y de equipo que tienen una ruta de ataque que conduce a un activo de nivel 0.



Para buscar un activo específico:

1. En el cuadro **Buscar**, escriba el nombre del activo.
2. En el cuadro **Activo**, haga clic en la flecha > para mostrar una lista desplegable de activos de nivel 0 y seleccione uno.

Tenable Identity Exposure actualiza la lista con los resultados correspondientes.

Para filtrar los activos de un dominio en particular:

1. Haga clic en el botón **n/n**.

Se abre el panel **Bosques y dominios**. Puede seguir cualquiera de los siguientes procedimientos:




- En el cuadro **Buscar**, escriba el nombre de un bosque o dominio.
- Seleccione la casilla **Expandir todo** y seleccione el bosque o dominio que quiera.

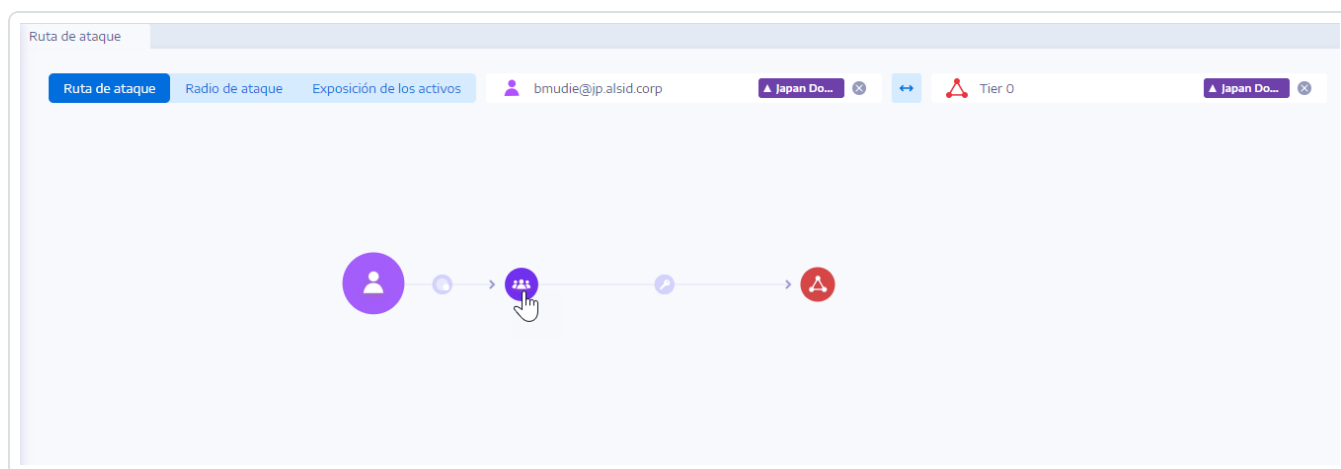
2. Haga clic en **Filtrar selección**.

Tenable Identity Exposure actualiza la lista de activos.

Para explorar la ruta de ataque:

- Al final de la línea del nombre del activo, haga clic en el ícono .

Tenable Identity Exposure abre la página “Ruta de ataque” desde ese activo a todos los activos de nivel 0. Para obtener más información, consulte [Ruta de ataque](#) y [Relaciones de ataque](#).




Tipos de nodos de ruta de ataque

La funcionalidad de rutas de ataque en Tenable Identity Exposure le muestra un gráfico donde aparecen las rutas de ataque abiertas a los atacantes dentro de su entorno de Active Directory. El gráfico consta de **aristas**, que representan las relaciones de ataque, y **nodos**, que representan objetos de Active Directory (LDAP o SYSVOL).








En la lista siguiente se describen todos los tipos de nodos posibles que puede esperar ver en los gráficos de rutas de ataque.

Tipo de nodo	Ubicación	Ícono	Descripción
--------------	-----------	-------	-------------





Usuario	LDAP		Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>user</code> , pero no <code>computer</code> .
Grupo	LDAP		Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>group</code> .
Dispositivo	LDAP		<p>Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>computer</code>, pero no <code>msDS-GroupManagedServiceAccount</code>.</p> <p>Su atributo <code>primaryGroupID</code> no es igual a 516 (DC) ni 521 (RODC).</p> <div style="border: 1px solid blue; padding: 5px;"><p>Nota: Para diferenciar los productos de Tenable, esta categoría se llama "Dispositivo" en lugar de "Equipo" para ser más genéricos.</p></div>
Unidad organizativa (OU)	LDAP		Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>organizationalUnit</code> . Evite la confusión entre los objetos de la clase <code>container</code> y el hecho de que cualquier objeto de Active Directory (AD) puede funcionar como contenedor, lo que le permite contener otros objetos.
Dominio	LDAP		Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>domainDNS</code> y ciertos atributos.
Controlador de dominio (DC)	LDAP		Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>computer</code> y su atributo <code>primaryGroupID</code> igual a 516 (por lo tanto, no es un RODC).
Controlador de dominio de solo lectura (RODC)	LDAP		Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>computer</code> y su atributo <code>primaryGroupID</code> igual a 521 (por lo tanto, no es un DC normal).



Política de grupo (GPC)	LDAP		Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>groupPolicyContainer</code> .
Archivo de GPO	SYSVOL		Archivo que se encuentra en el recurso compartido de SYSVOL de un GPO específico (por ejemplo, “\\ejemplo.net\sysvol\ejemplo.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\{Machine,User}\Preferences\ScheduledTasks\ScheduledTasks.xml”).
Carpeta de GPO	SYSVOL		Carpeta que se encuentra en el recurso compartido de SYSVOL de un GPO específico. Hay una para cada GPO (por ejemplo, “\\ejemplo.net\sysvol\ejemplo.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\Machine\Scripts\Startup”).
Cuenta de servicios administrada por grupo (gMSA)	LDAP		Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>msDS-GroupManagedServiceAccount</code> .
Almacén Enterprise NTAAuth	LDAP		Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>certificationAuthority</code> .
Plantilla de certificados de la PKI	LDAP		Objeto de LDAP cuyo atributo <code>objectClass</code> contiene la clase <code>pKICertificateTemplate</code> .
Entidad de seguridad sin resolver	LDAP		Objeto de LDAP cuyo atributo <code>objectSid</code> o <code>DistinguishedName</code> se usa en algún momento al crear relaciones, pero para el cual hay un objeto de entidad de seguridad de LDAP correspondiente desconocido (caso




			<p>clásico de "SID sin resolver").</p> <p>También falta información sobre el tipo específico de entidad de seguridad (usuario, equipo, grupo, etc.) asociado; solo se conoce su identificador de seguridad o nombre distintivo.</p>
Identidad especial	LDAP		<p>Windows y Active Directory usan identidades conocidas internamente. Estas identidades funcionan de manera similar a los grupos, pero AD no las declara como tales. Para obtener más información, consulte Grupos de identidades especiales.</p>
Otros			<p>Actualmente, todos los objetos de AD o SYSVOL que no entran en las categorías mencionadas.</p>

Registros de actividad

Los registros de actividad en Tenable Identity Exposure le permiten ver los rastros de todas las actividades que tuvieron lugar en la plataforma de Tenable Identity Exposure relacionadas con direcciones IP, usuarios o acciones específicas.

Nota: Debido a limitaciones técnicas, los registros de actividad relativos a vistas específicas, como "Gestión de inquilinos" (incluida la adición, edición o eliminación), no están visibles actualmente.

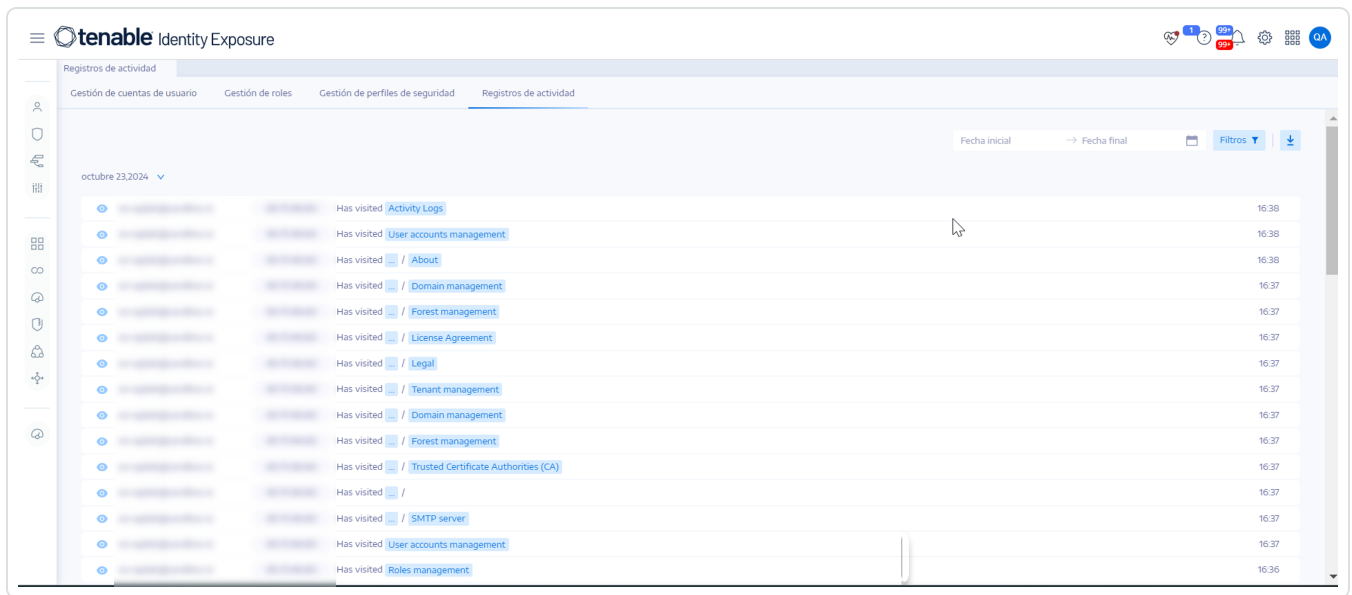
Para ver los registros de actividad:

1. En Tenable Identity Exposure, haga clic en el ícono **Cuentas**  en el menú de navegación izquierdo.

Aparece el panel **Gestión de cuentas de usuario**.

2. Seleccione la pestaña **Registros de actividad**.

Se abre el panel "Registros de actividad".

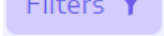


Para mostrar los registros de actividad de un período específico:

1. En la parte superior del panel de registros de actividad, haga clic en el selector de fechas.
2. Seleccione una fecha inicial y una fecha final para el período que desee.
3. (Opcional) Utilice la barra de desplazamiento para seleccionar la hora (valor predeterminado: hora actual).
4. Haga clic en **Aceptar**.

Tenable Identity Exposure muestra el registro de actividad para ese período.

Para filtrar los registros de actividad:

1. En la parte superior del panel de registros de actividad, haga clic en el botón . Aparece el panel **Filtros**.
2. Haga clic en ">" en los siguientes cuadros:
 - Dirección IP
 - Usuario
 - Acción



3. Haga clic en **Validar**.


Tenable Identity Exposure muestra el registro de actividad del filtro que definió.

Para borrar los filtros:

- Al final del panel **Filtros**, haga clic en **Borrar filtros**.

Tenable Identity Exposure muestra el registro de actividad sin filtrar.

Para exportar los registros de actividad:

- Al principio del panel de registros de actividad, haga clic en el ícono .

Tenable Identity Exposure descarga el registro de actividad en formato CSV en el equipo.

Definiciones de entidades privilegiadas

Tenable Identity Exposure utiliza el concepto de entidades “**privilegiadas**” en varios indicadores de exposición, indicadores de ataque y otras funcionalidades. La definición de “entidades privilegiadas” difiere entre Active Directory y Entra ID:

Active Directory

Las entidades privilegiadas pueden abarcar **usuarios privilegiados, cuentas de equipo privilegiadas, cuentas de servicio privilegiadas, grupos privilegiados, entidades de seguridad privilegiadas**, etc. Las entidades privilegiadas incluyen a los usuarios Sistema (local) y KRBTGT (ticket de concesión de tickets de Kerberos) y todos los miembros directos o indirectos (transitivos) de los siguientes grupos privilegiados nativos, que se identifican de forma interna mediante su [identificador relativo o identificador de seguridad](#) conocido, independientemente de sus nombres.

- Operadores de cuentas
- Administradores
- Operadores de copia de seguridad
- Publicadores de certificados
- Administradores de dominio



- Controladores de dominio
- Administradores de empresas
- Controladores de dominio empresariales
- Administradores empresariales de claves
- Controladores de dominio empresariales de solo lectura
- Propietarios del creador de directivas de grupo
- Administradores de claves
- Operadores de impresión
- Controladores de dominio de solo lectura
- Replicadores
- Administradores de esquema
- Operadores de servidor

Entra ID

- Un **derecho** o **permiso privilegiado** es aquel que [Microsoft identifica como tal](#).
- Un **rol privilegiado** es un rol de Entra que contiene al menos un permiso privilegiado [según lo definido por Microsoft](#).
- Las **entidades privilegiadas** (usuarios, grupos o entidades de servicio) son aquellas asignadas de forma directa o indirecta (transitivamente a través de un grupo asignable a un rol) a cualquier rol privilegiado de Entra.



Configuración y administración de Tenable Identity Exposure

Las opciones y funcionalidades que se describen en esta sección están dirigidas a administradores y usuarios avanzados que buscan personalizar, optimizar y mantener su instalación o implementación de Tenable Identity Exposure .

Aquí encontrará instrucciones especializadas sobre temas como la gestión de Active Directory, la configuración de la implementación de indicadores de ataque, las opciones de autenticación, las cuentas de usuario, los perfiles de seguridad, los roles, los bosques, los dominios y las alertas. En esta sección también se abordan la ejecución de verificaciones de estado, el uso del Centro de informes, la integración en Microsoft Entra ID (anteriormente Azure AD), las licencias y la resolución de problemas.

Para encontrar información relacionada con una tarea en particular, haga clic en los temas pertinentes en el panel de menú a la izquierda de la pantalla.

Permiso: estas tareas requieren privilegios de acceso administrativo.

Configuración de Active Directory

Tenable Identity Exposure requiere cierta configuración en la instancia de Active Directory supervisada para permitir que ciertas características funcionen:

- [Acceder a objetos o contenedores de AD](#)
- [Acceso a Análisis con privilegios](#)
- [Implementación de indicadores de ataque](#)

Acceder a objetos o contenedores de AD

Nota: Esta sección solo se aplica a una licencia de Tenable Identity Exposure para el módulo de indicadores de exposición.

Tenable Identity Exposure no requiere privilegios administrativos para encargarse de la supervisión de la seguridad.



Este enfoque se basa en la capacidad de la cuenta de usuario que Tenable Identity Exposure usa para leer todos los objetos de Active Directory que se almacenan en un dominio (incluidas las cuentas de usuario, las unidades organizativas, los grupos, etc.).

De manera predeterminada, la mayoría de los objetos tienen acceso de lectura para el grupo "Usuarios del dominio" que usa la cuenta de servicio de Tenable Identity Exposure. Sin embargo, tiene que configurar manualmente algunos contenedores para permitir el acceso de lectura a la cuenta de usuario de Tenable Identity Exposure.

En la siguiente tabla se detallan los objetos y contenedores de Active Directory que requieren configuración manual para el acceso de lectura en cada dominio que Tenable Identity Exposure supervisa.

Ubicación del contenedor	Descripción
CN=Deleted Objects,DC=<DOMAIN>,DC=<TLD>	Un contenedor que hospeda objetos eliminados.
CN=Password Settings Container,CN=System,DC=<DOMAIN>,DC=<TLD>	(Opcional) Un contenedor que hospeda objetos de configuración de contraseñas.

Para conceder acceso a objetos y contenedores de AD:

- En la consola de PowerShell del controlador de dominio, ejecute los siguientes comandos para otorgar acceso a objetos o contenedores de Active Directory:

Nota: Debe ejecutar estos comandos en cada dominio que Tenable Identity Exposure supervisa.

```
#Set Service Account $serviceAccount = "<SERVICE_ACCOUNT>" #Don't Edit after here $domain =  
Get-ADDomain @($domain.DeletedObjectsContainer, "CN=Password Settings  
Container,$($domain.SystemsContainer)") | ForEach-Object { & dscls $_ /takeownership & dscls  
$_ /g "$($serviceAccount):LCRP" /I:T }
```

donde <__SERVICE_ACCOUNT__> hace referencia a la cuenta de servicio que Tenable Identity Exposure usa.



Como alternativa, si PowerShell no está disponible, también puede ejecutar estos comandos para cada contenedor:

```
dsacIs "<__CONTAINER__>" /takeownership  
dsacIs "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
```

donde:

- <__CONTAINER__> hace referencia al contenedor que requiere acceso.
- <__SERVICE_ACCOUNT__> hace referencia a la cuenta de servicio que Tenable Identity Exposure usa.

Acceso a Análisis con privilegios

La funcionalidad opcional Análisis con privilegios requiere privilegios administrativos. Debe asignar permisos para la cuenta de servicio que Tenable Identity Exposure usa.

Para obtener más información, consulte [Análisis con privilegios](#).

Nota: Debe asignar permisos en cada dominio donde habilite Análisis con privilegios.

Para asignar permisos usando la línea de comandos:

Requisito: Para asignar permisos, necesita una cuenta con derechos de Administrador de dominio o equivalente.

- En la interfaz de la línea de comandos del controlador de dominio, ejecute el siguiente comando para agregar ambos permisos:

```
dsacIs "<__DOMAIN_ROOT__>" /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
```

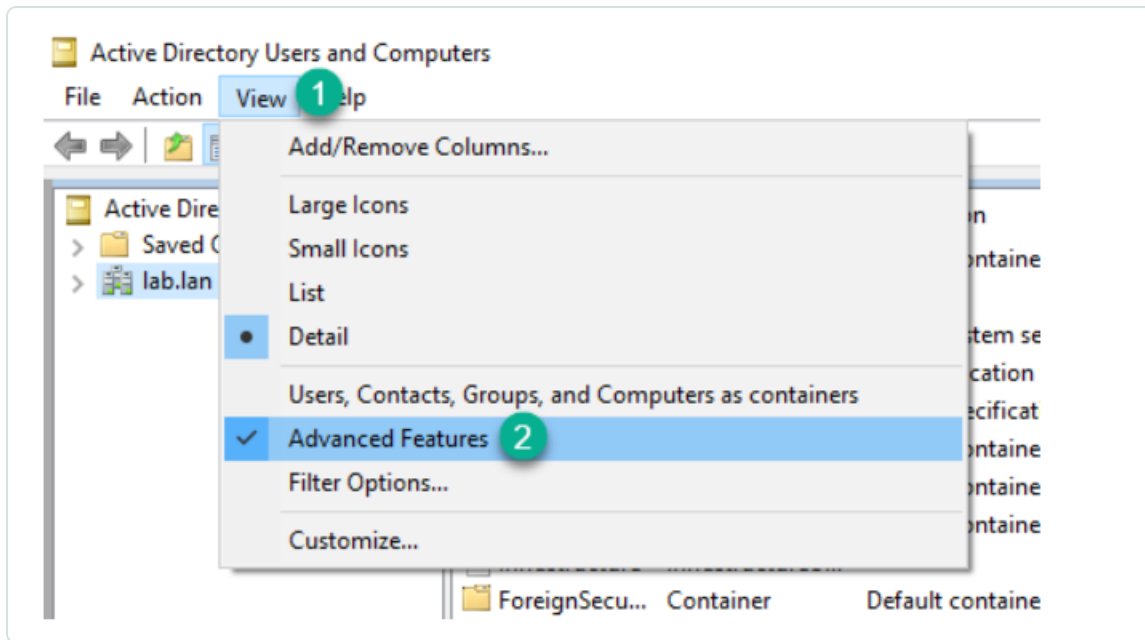
Donde:

- <__DOMAIN_ROOT__> hace referencia al nombre distintivo de la raíz del dominio.
Ejemplo: DC=<DOMAIN>,DC=<TLD>.

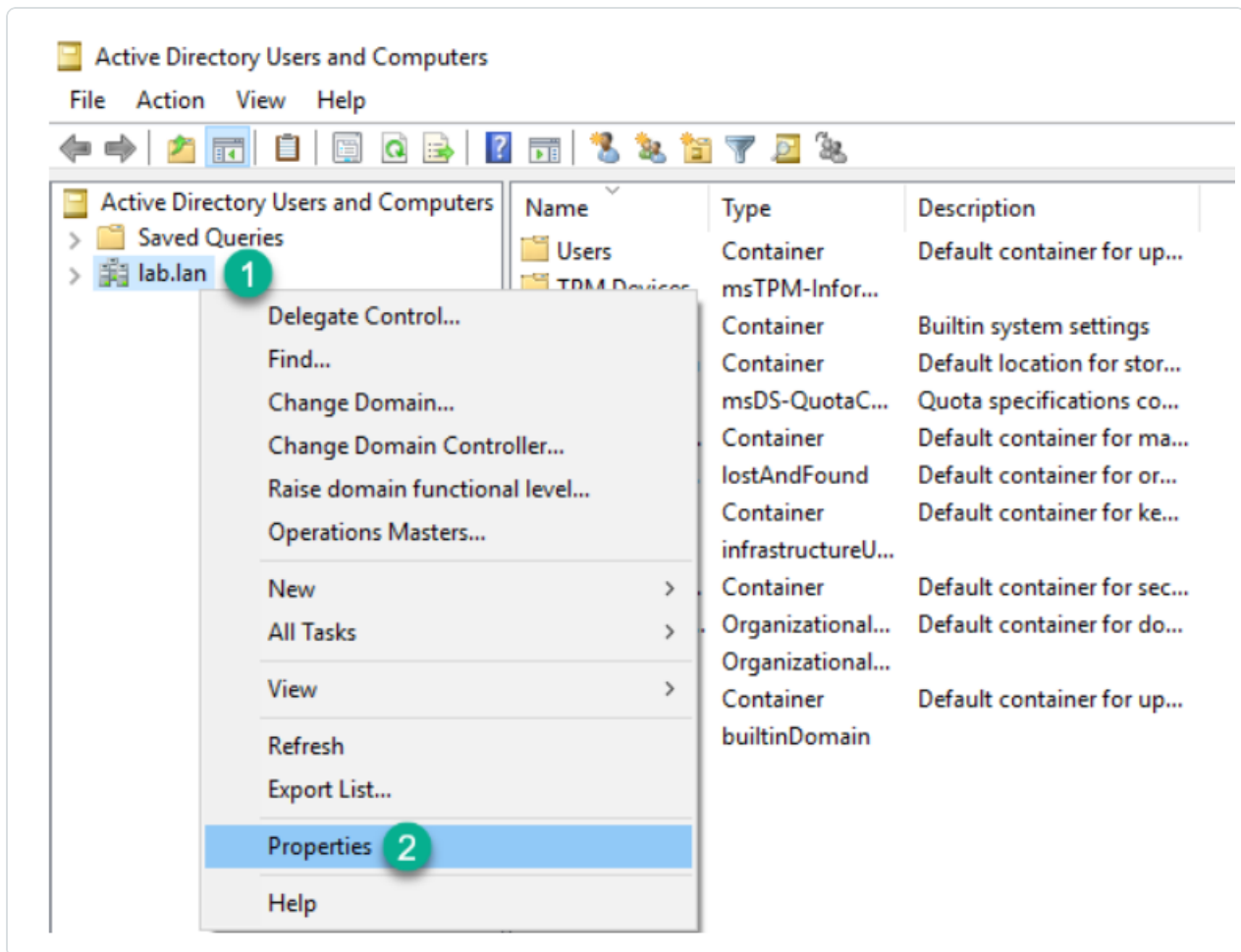
- <__SERVICE_ACCOUNT__> hace referencia a la cuenta de servicio que Tenable Identity Exposure usa. Ejemplo: DOMAIN\tenablelead.

Para asignar permisos mediante la interfaz gráfica de usuario:

1. Desde el menú **Inicio** de Windows, abra **Usuarios y equipos de Active Directory**.
2. En el menú **Ver**, seleccione **Características avanzadas**.

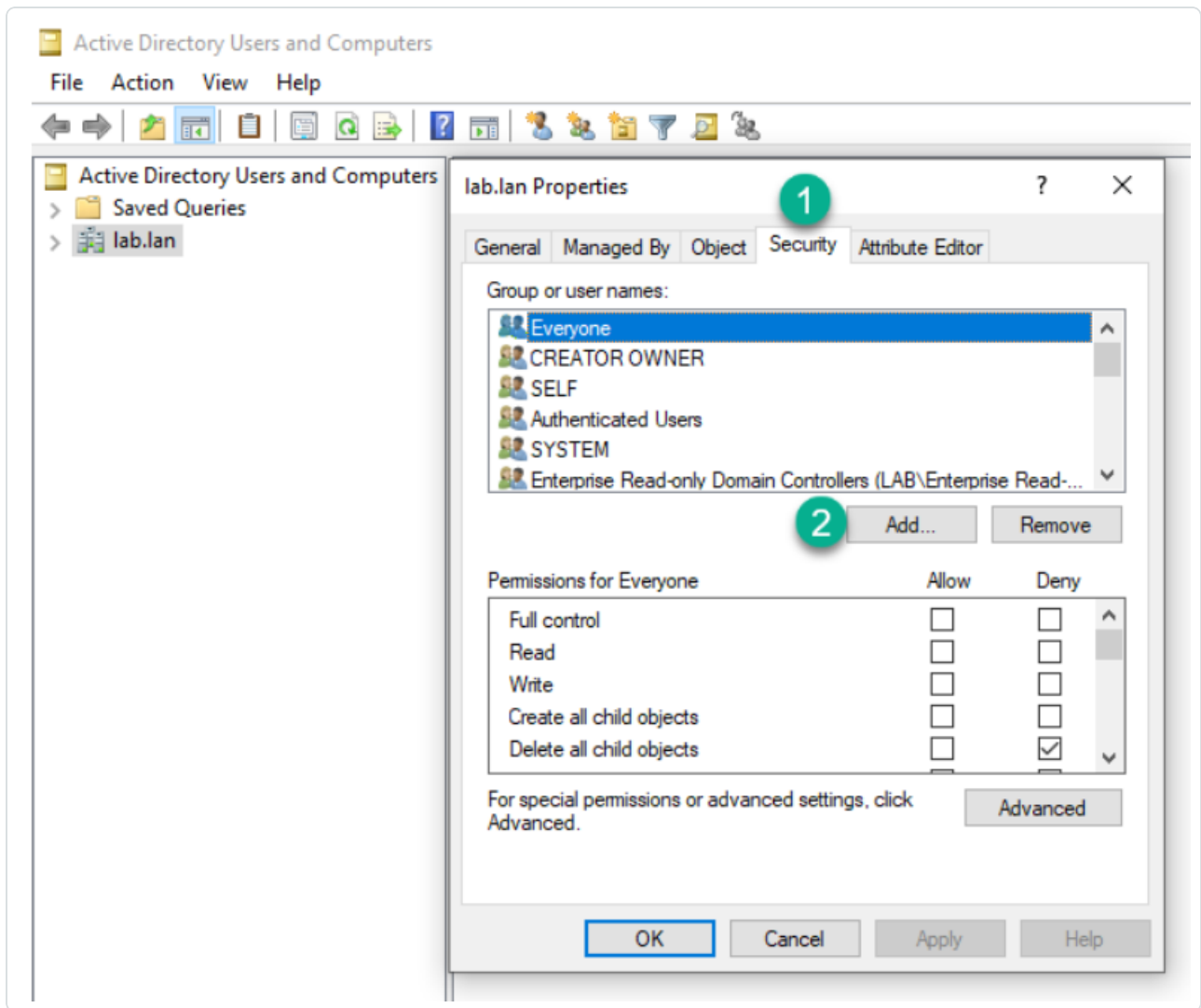


3. Haga clic con el botón derecho en la raíz del dominio y seleccione **Propiedades**.



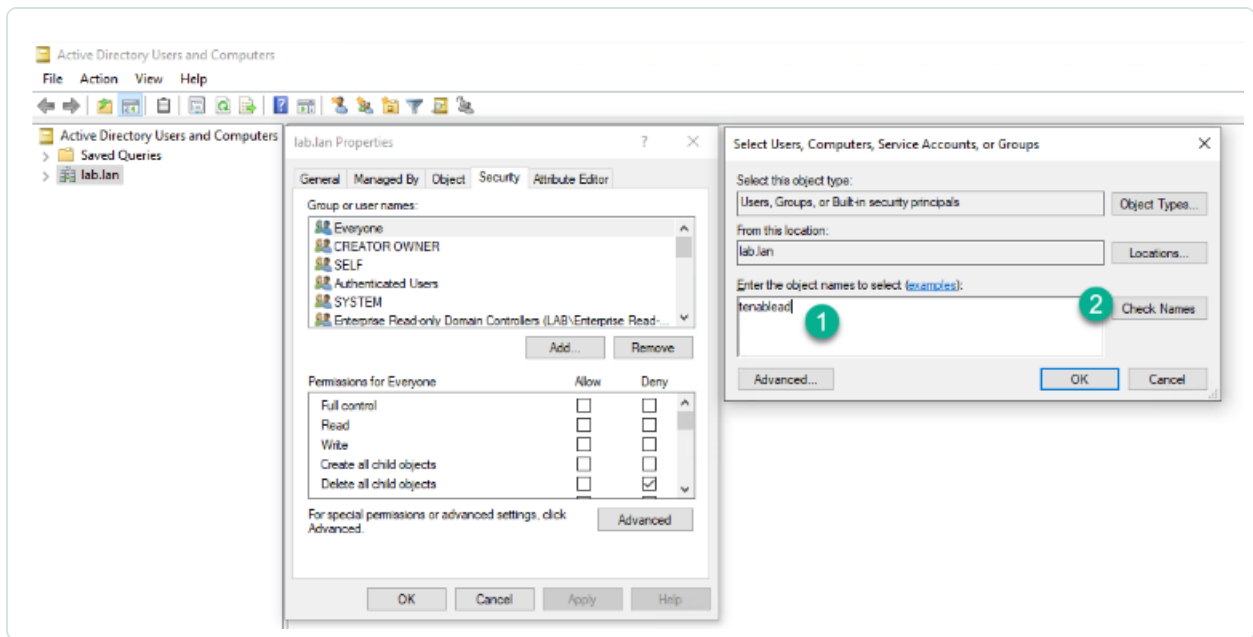
Se abre el panel de propiedades de la raíz del dominio.

4. Haga clic en la pestaña **Seguridad** y luego en **Agregar**.

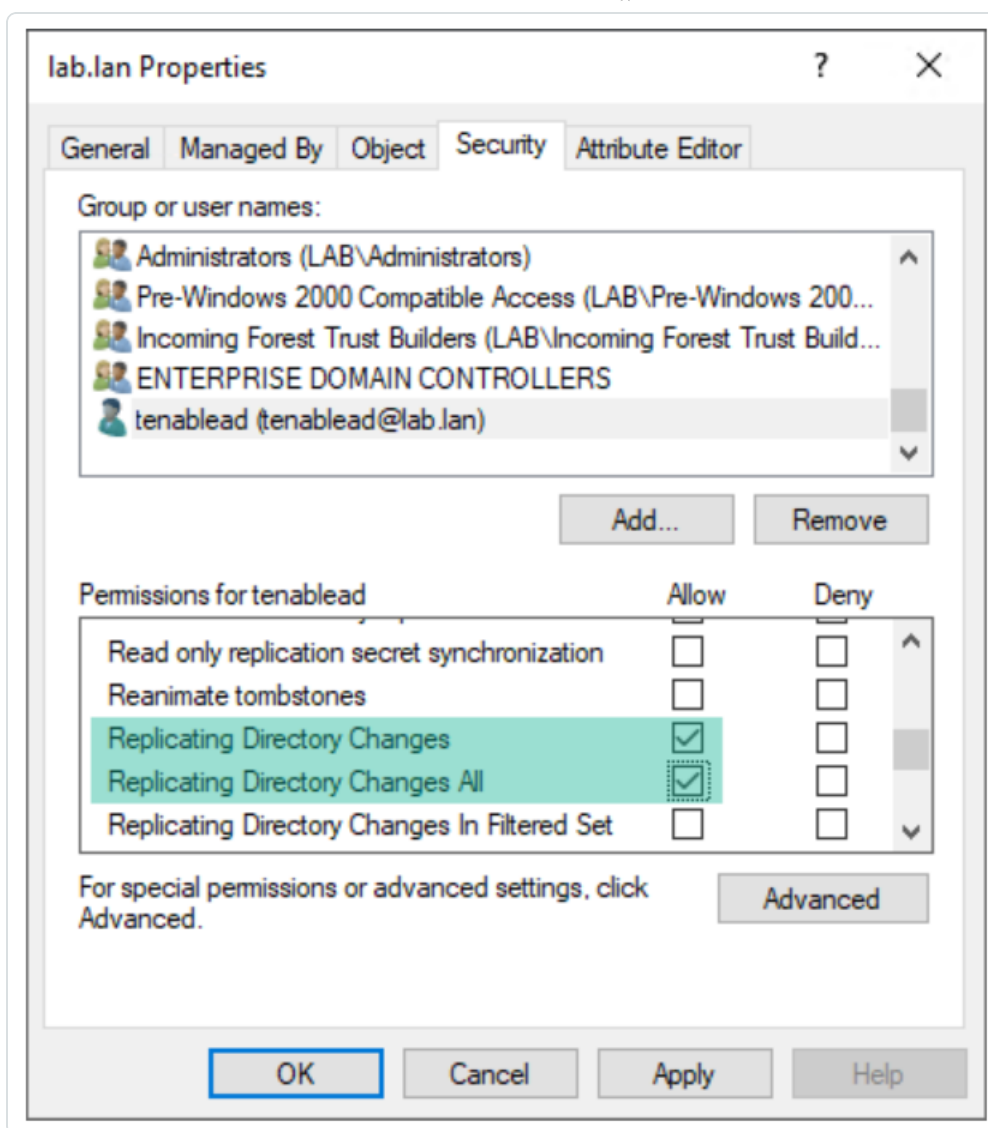


5. Busque la cuenta de servicio de Tenable Identity Exposure:

Nota: En un entorno de bosque con varios dominios, la cuenta de servicio puede estar en otro dominio de Active Directory.



6. Desplácese hacia abajo por la lista y anule la selección de todos los permisos establecidos de manera predeterminada.
7. En la columna **Permitir**, seleccione permisos tanto para *Replicación de cambios de directorio* como para *Replicación de todos los cambios de directorio*.



8. Haga clic en **Aceptar**.

Notas importantes

Tenable Identity Exposure solo requiere una cuenta de servicio por bosque, por lo que, cuando asigna permisos en un dominio, es posible que tenga que **buscar la cuenta de servicio de otro dominio**.

Tiene que asignar permisos adicionales **en el nivel de raíz del dominio**. Active Directory no admite permisos que se asignan a una unidad organizativa o a un usuario específico (por ejemplo, para restringir Análisis con privilegios a la unidad organizativa o al usuario) y, por lo tanto, estos no tienen ningún efecto.

Estos permisos otorgan a la cuenta de servicio de Tenable Identity Exposure mucho más poder sobre el dominio de Active Directory. Luego tiene que considerarla como **una cuenta privilegiada (nivel 0)** y



protegerla de forma similar a una cuenta de administrador de dominio. Para conocer el procedimiento completo, consulte [Proteger cuentas de servicio](#).

Implementación de indicadores de ataque

Nota: Esta información solo se aplica a las licencias que se benefician del módulo de indicadores de ataque.

Los **indicadores de ataque** (IoA) de Tenable Identity Exposure le brindan la capacidad de detectar ataques a su instancia de Active Directory (AD). Cada IoA requiere políticas de auditoría específicas que el script de instalación habilita de manera automática. Para obtener una lista completa de los IoA de Tenable Identity Exposure y su implementación, consulte [Tenable Identity Exposure Indicators of Attack Reference Guide](#) (Guía de referencia de indicadores de ataque de Tenable Identity Exposure) en el portal de descargas de Tenable.

Indicadores de ataque y Active Directory

Tenable Identity Exposure funciona como solución no intrusiva que supervisa una infraestructura de Active Directory sin implementar agentes y con un cambio de configuración mínimo en el entorno.

Tenable Identity Exposure usa una cuenta de usuario normal sin permisos administrativos para conectarse a las API estándar para su funcionalidad de supervisión de la seguridad.

Tenable Identity Exposure usa los mecanismos de replicación de Active Directory para recuperar la información pertinente, lo que solo genera costos de ancho de banda limitados entre el PDC de cada dominio y Directory Listener de Tenable Identity Exposure.

Para detectar de manera eficiente incidentes de seguridad mediante indicadores de ataque, Tenable Identity Exposure usa la información de Seguimiento de eventos para Windows (ETW) y los mecanismos de replicación disponibles en cada controlador de dominio. Para recopilar este conjunto de información, implemente un objeto de política de grupo (GPO) dedicado mediante un script desde Tenable Identity Exposure como se describe en [Instalar indicadores de ataque](#).

Este GPO activa un cliente de escucha de registros de eventos mediante las API EvtSubscribe de Windows en todos los controladores de dominio que escriben en el volumen del sistema (SYSVOL) para beneficiarse del motor de replicación de AD y la capacidad de Tenable Identity Exposure de escuchar eventos de SYSVOL. El GPO crea un archivo en SYSVOL para cada controlador de dominio y vacía su contenido periódicamente.



Para iniciar la supervisión de seguridad, Tenable Identity Exposure tiene que comunicarse con las API de directorio estándar de Microsoft.



Controlador de dominio

Tenable Identity Exposure solo requiere comunicación con el emulador del controlador de dominio principal (PDCe) mediante los protocolos de red que se describen en [Matriz de flujos de red](#).

En caso de que se supervisen varios dominios o bosques, Tenable Identity Exposure tiene que acceder al PDCe de cada dominio. Para lograr el mejor rendimiento, Tenable recomienda hospedar Tenable Identity Exposure en una red física cerca del PDCe que se va a supervisar.

Cuenta de usuario

Tenable Identity Exposure se autentica en la infraestructura supervisada mediante una cuenta de usuario que no es de administrador para acceder al flujo de replicación.

Un usuario simple de Tenable Identity Exposure puede acceder a todos los datos recopilados. Tenable Identity Exposure no accede a atributos secretos, como credenciales, hashes de contraseñas o claves de Kerberos.

Tenable recomienda que cree una cuenta de servicio que sea miembro del grupo "Usuarios de dominio" de la siguiente manera:



- La cuenta de servicio se encuentra en el dominio principal supervisado.
- La cuenta de servicio se encuentra en cualquier unidad organizativa (OU), de preferencia donde se crean otras cuentas de servicio de seguridad.
- La cuenta de servicio tiene una pertenencia al grupo de usuarios estándar (como miembro del grupo predeterminado de AD "Usuarios de dominio").

Antes de empezar

- Revise las limitaciones y los posibles efectos de la instalación de los loA, como se describe en [Cambios técnicos e impacto potencial](#).
- Compruebe que el DC tenga instalados y disponibles los módulos de PowerShell para Active Directory y GroupPolicy.

Para ello, ejecute el siguiente comando de PowerShell en la máquina de destino (controlador de dominio) donde tiene pensado implementar el módulo de loA:

```
if (-not (Get-Module -ListAvailable -Name GroupPolicy)) {  
    Write-Error "The GroupPolicy module is not installed or not available on this machine. This  
is a requirement for this script and the IOAs to run, please install it and run this script  
again."  
}
```

Si aparece un error en la consola, se debe a que este requisito no está validado en el entorno actual.

- Compruebe que el DC tenga habilitada la funcionalidad RSAT-DFS-Mgmt-Con de las herramientas del sistema de archivos distribuido para que el script de implementación pueda comprobar el estado de la replicación, ya que no puede crear un GPO mientras el DC se está replicando.
- Tenable Identity Exposure recomienda que instale o actualice los loA durante las horas de menor actividad, con el fin de limitar las perturbaciones en la plataforma.
- Compruebe los permisos. Para instalar los loA, debe tener un rol de usuario con los siguientes permisos:



- En **Entidades de datos**, acceso “Leer” para:
 - Todos los indicadores de ataque
 - Todos los dominios
- En **Entidades de interfaz**, acceso para:
 - Gestión > Sistema > Configuración
 - Gestión > Sistema > Configuración > Servicios de aplicación > Indicadores de ataque
 - Gestión > Sistema > Configuración > Servicios de aplicación > Indicadores de ataque > Descargar archivo de instalación

Para obtener más información sobre los permisos basados en roles, consulte [Establecer permisos para un rol](#).

Consulte también

- [Instalar indicadores de ataque](#)
- [Script de instalación de indicadores de ataque](#)
- [Cambios técnicos e impacto potencial](#)
- [Instalar Microsoft Sysmon](#), una herramienta del sistema de Windows que algunos de los indicadores de ataque de Tenable Identity Exposure requieren para obtener datos pertinentes del sistema.
- [Solucionar problemas de indicadores de ataque](#)

Instalar indicadores de ataque

Rol de usuario obligatorio: usuario de la organización con permiso para modificar la configuración de los indicadores de ataque en Tenable Identity Exposure. Para obtener más información, consulte [Establecer permisos para un rol](#).

El módulo de indicadores de ataque (IoA) de Tenable Identity Exposure requiere que ejecute un script de instalación de PowerShell con una cuenta administrativa que pueda crear y vincular un



nuevo objeto de política de grupo (GPO) a una unidad organizativa (OU). Puede ejecutar este script desde cualquier máquina unida a su dominio de Active Directory que Tenable Identity Exposure supervisa y que puede acceder a los controladores de dominio a través de la red.

Nota: Tiene que volver a implementar el script de instalación de loA después de cada nueva publicación de una versión principal de Tenable Identity Exposure.

Nota: La versión recomendada de PowerShell es la 5.1.

Solo tiene que ejecutar este script de instalación una vez para cada dominio de AD, ya que el GPO creado implementa automáticamente el cliente de escucha de eventos en todos los controladores de dominio (DC) existentes y nuevos.

Además, habilitar la opción “Actualizaciones automáticas” evita tener que volver a ejecutar el script de instalación, incluso si cambia la configuración de los loA.

Para configurar dominios para los loA:

1. En Tenable Identity Exposure, haga clic en **Sistema** en la barra de menú de la izquierda y seleccione la pestaña **Configuración**.

Aparece el panel **Configuración**.

2. Haga clic en **Indicadores de ataque**.

Aparece el panel de configuración de los loA.

The screenshot shows the Tenable Identity Exposure web interface. The left sidebar contains a navigation menu with categories like 'SERVICIOS DE APLICACIÓN', 'MOTOR DE ALERTAS', and 'INFORMES'. The main content area is titled 'Configuración de dominios' and includes sections for 'Configuración de dominios', 'Demora en la búsqueda', and 'Configuración de indicadores de ataque'. The 'Configuración de indicadores de ataque' section features a table with columns for various domains and rows for different attack indicators. Each cell in the table contains a blue checkmark, indicating that all indicators are enabled for all domains.


Nombre del ataque	ALSID, CORP Fore...	Japan Domain @...	ALSID	INAU Forest	TR/INAU	KHLAB forest	KHLAB	TCORP Forest	TCORP Domain
<input checked="" type="checkbox"/> Cambio sospechoso de contraseña de contr...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> DCShadow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> DCsync	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Explotación de Zerologon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Extracción de claves de copia de segurid...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Extracción de NTDS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Golden Ticket	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Petrotam	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Suplantación de identidad de SAMAccountN...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Volcado de credenciales del sistema oper...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Explotación de DnsAdmins	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Actualización de contraseña	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>




3. En **(1) Configuración de dominios**, haga clic en **Ver el procedimiento**.

Se abre una ventana "Procedimiento".

Procedimiento

 **¿Actualizaciones automáticas en el futuro?**

Para evitar tener que reconfigurar manualmente los dominios con cada modificación futura, se recomienda habilitar las actualizaciones automáticas. [Más información](#)


 Tenable.ad aplicará automáticamente los futuros cambios de configuración.
Siga el procedimiento a continuación a fin de configurar los dominios para las actualizaciones automáticas.

1. Descargue el archivo "Register-TenableIOA.ps1". [Descargar](#)

2. Descargue el archivo de configuración de indicadores de ataque para todos los dominios "TadIoaConfig-AllDomains.json". [Descargar](#)

3. Ejecute los siguientes comandos de PowerShell para configurar los dominios:

```
./Register-TenableIOA.ps1 -DomainControllerAddress apjlab-afad-dc-.jp.alsid.corp -TenableServiceAccount svc.alsid@alsid.corp -ConfigurationFileLocation ./TadIoaConfig-AllDomains.json
./Register-TenableIOA.ps1 -DomainControllerAddress apjlab-dc.alsid.corp -TenableServiceAccount svc.alsid@alsid.corp -ConfigurationFileLocation ./TadIoaConfig-AllDomains.json
./Register-TenableIOA.ps1 -DomainControllerAddress tk-dcl.tk.jv4u.com -TenableServiceAccount svc.tenablead@tk.jv4u.com -ConfigurationFileLocation ./TadIoaConfig-AllDomains.json
./Register-TenableIOA.ps1 -DomainControllerAddress dc-vm.tenable.ad -TenableServiceAccount svc.tenablead@tenable.ad -ConfigurationFileLocation ./TadIoaConfig-AllDomains.json
./Register-TenableIOA.ps1 -DomainControllerAddress dc01.tcorp.local -TenableServiceAccount svc.alsid_priv@tcorp.local -ConfigurationFileLocation ./TadIoaConfig-AllDomains.json
```




4. En **¿Actualizaciones automáticas en el futuro?:**

- La opción predeterminada **Habilitado** permite que Tenable Identity Exposure actualice automáticamente la configuración de los loA siempre que la modifique en Tenable Identity Exposure en el futuro. Esto también garantiza un análisis de seguridad continuo.
- Si desactiva esta opción, aparecerá un mensaje para pedirle que la active para recibir actualizaciones automáticas en el futuro. Haga clic en **Ver el procedimiento** y cambie a **Habilitado**.

5. Haga clic en **Descargar** para descargar el script que se ejecutará para cada dominio (Register-TenableIOA.ps1).

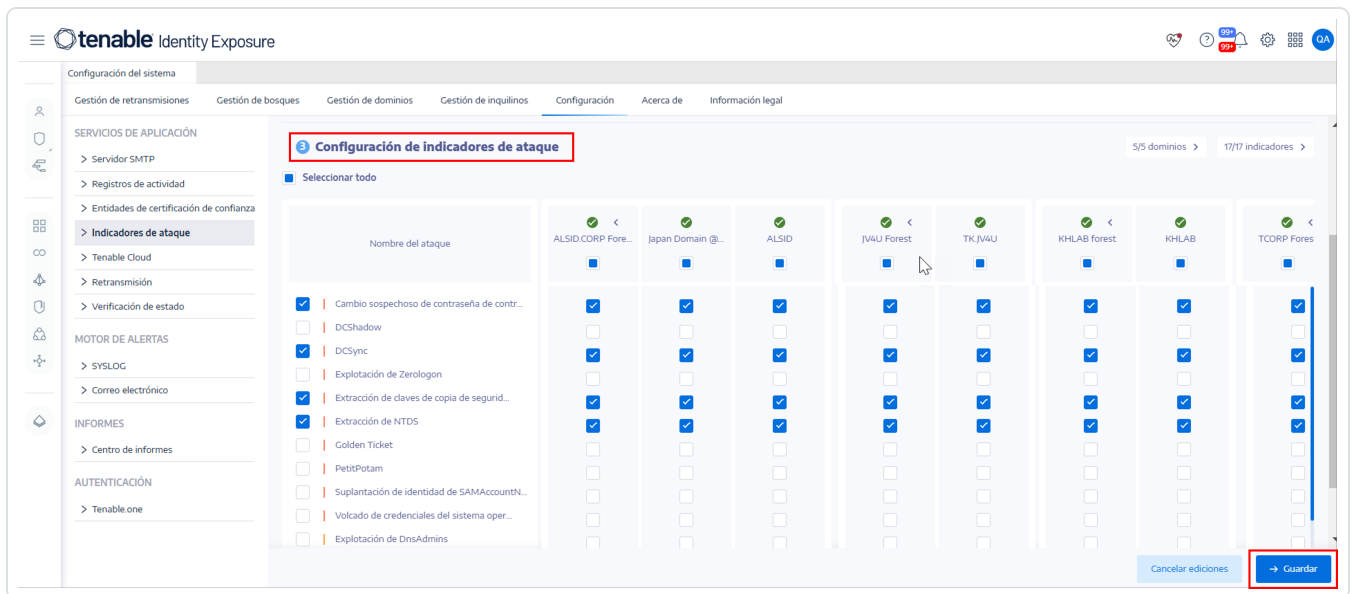


6. Haga clic en **Descargar** para descargar el archivo de configuración para los dominios (TadIoaConfig-AllDomains.json).
7. Haga clic en  para copiar el comando de PowerShell para configurar los dominios.
8. Haga clic fuera de la ventana "Procedimiento" para cerrarla.
9. Abra un terminal de PowerShell con derechos administrativos y ejecute los comandos para configurar los controladores de dominio para los loA.

Nota: La cuenta de servicio que se usa para instalar los loA y consultar los dominios debe tener permisos de escritura en la carpeta de GPO de Tenable Identity Exposure (anteriormente, Tenable.ad). El script de instalación agrega este permiso de manera automática. Si quita este permiso, Tenable Identity Exposure muestra un mensaje de error y las actualizaciones automáticas ya no funcionan. Para obtener más información, consulte [Script de instalación de indicadores de ataque](#).

Para configurar los loA:

1. En el panel de configuración de loA, en **Configuración de indicadores de ataque**, seleccione los loA que quiera en la configuración.



The screenshot shows the Tenable Identity Exposure web interface. The main content area is titled "Configuración de indicadores de ataque" and displays a table of attack indicators for five domains: ALSIDCORP Fore..., Japan Domain @..., ALSID, JV4U Forest, TKJV4U, KHLAB forest, KHLAB, and TCORP Fores. The table has columns for the domain name and a grid of checkboxes for each indicator. The indicators listed are: Cambio sospechoso de contraseña de contr..., DCShadow, DCSync, Explotación de Zerologon, Extracción de claves de copia de segurid..., Extracción de NTDS, Golden Ticket, PetitPotam, Suplantación de identidad de SAMAccountN..., Volcado de credenciales del sistema oper..., and Explotación de DnsAdmins. The "Guardar" button is highlighted with a red box in the bottom right corner.

Sugerencia: El indicador de ataque (loA) **Explotación de Zerologon** data de 2020. Si todos los controladores de dominio (DC) recibieron actualizaciones en los últimos tres años, están protegidos contra esta vulnerabilidad. Para conocer los parches necesarios para proteger los DC frente a esta



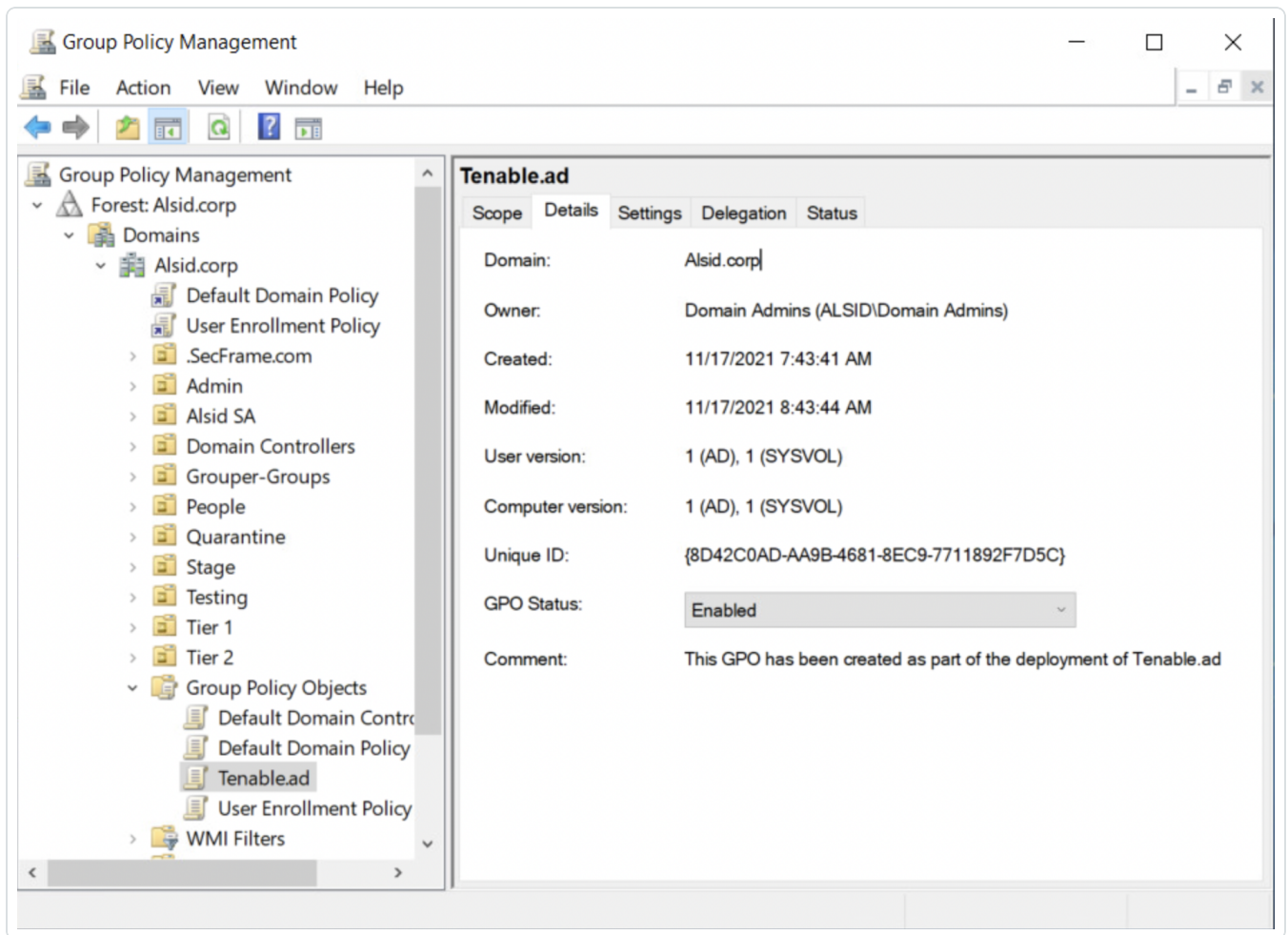
vulnerabilidad, consulte la información en [Netlogon Elevation of Privilege Vulnerability](#) (texto en inglés) de Microsoft. Una vez que haya confirmado la seguridad de los DC, puede desactivar de forma segura este loA para evitar alertas innecesarias.

2. Haga clic en **Guardar**.

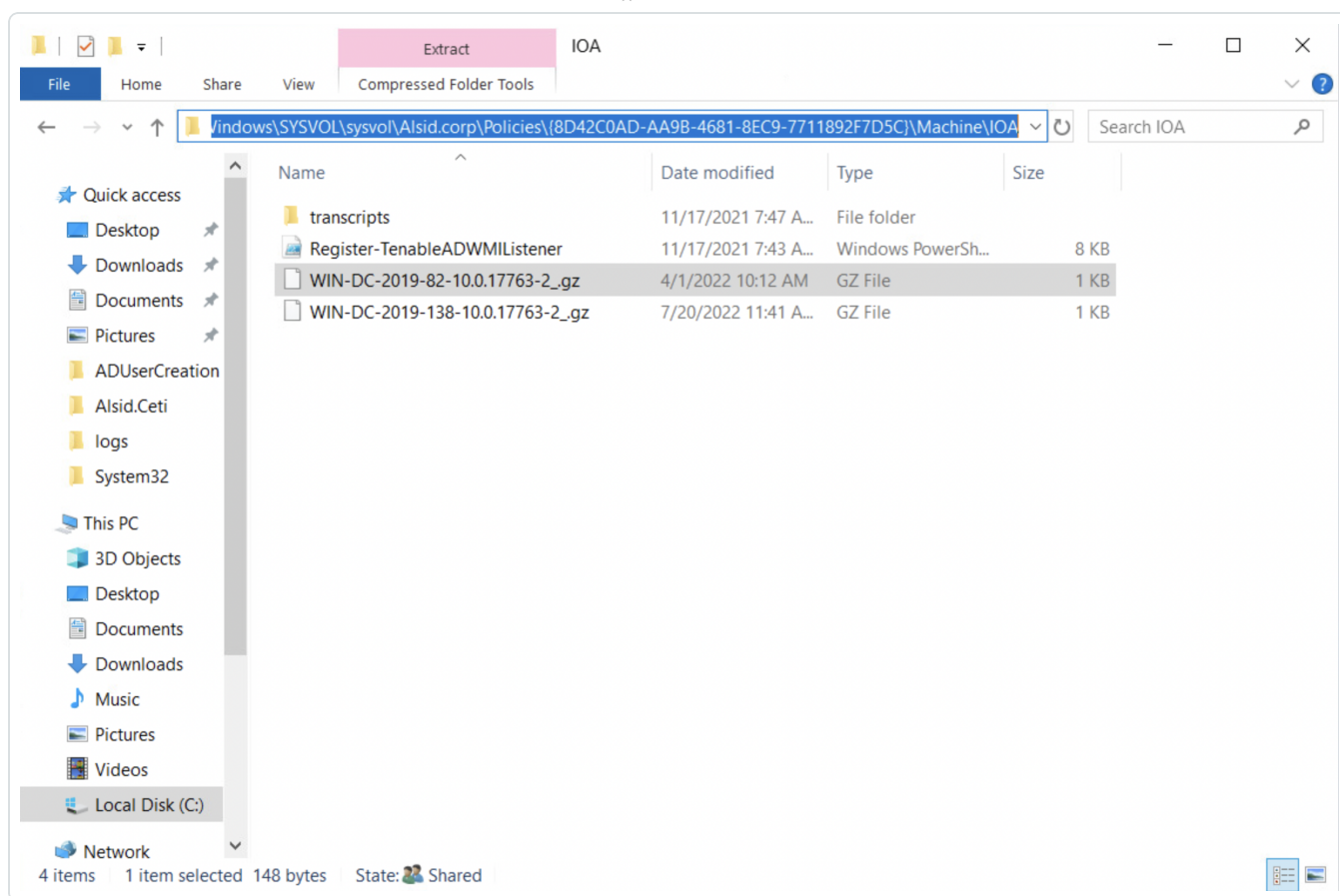
- Si habilitó **¿Actualizaciones automáticas en el futuro?**, Tenable Identity Exposure guarda y actualiza automáticamente la nueva configuración. Espere unos minutos para que esta actualización surta efecto.
- Si no habilitó **¿Actualizaciones automáticas en el futuro?**, aparecerá una ventana "Procedimiento" como guía [Para configurar dominios para los loA:](#)

Para comprobar la instalación de los loA:

1. En Administración de directivas de grupo, compruebe que el nuevo GPO de Tenable Identity Exposure exista y se vincule con la unidad organizativa `Controladores de dominio`:



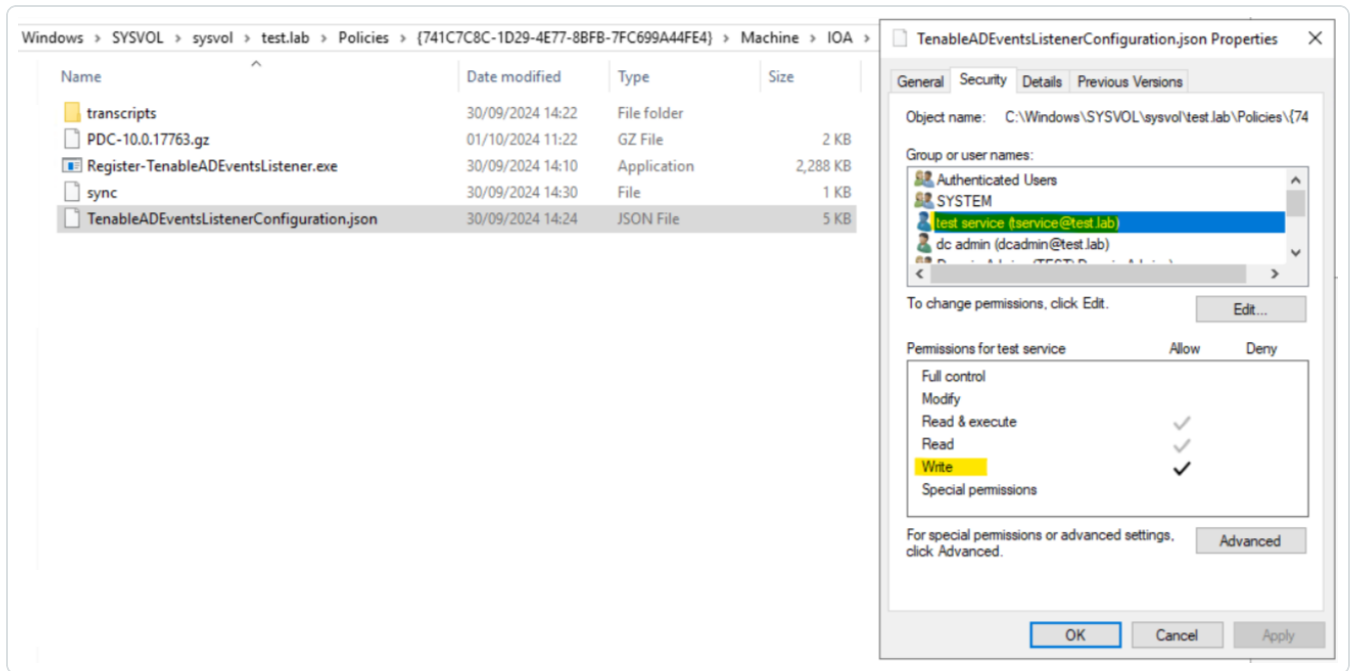
2. Vaya a la ruta `C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{GUID}\Machine\IOA` y compruebe que el archivo `.gz` exista para **todos los controladores de dominio** antes de probar los loA:



Para comprobar el acceso al permiso “Escribir” para la cuenta de servicio de Tenable Identity Exposure:

1. En el administrador de archivos, vaya a `\\<NOMBRE-DNS>\sysvol\<NOMBRE-DNS>\Policies\{<ID-GPO>\Machine\`.
2. Haga clic con el botón derecho en el archivo `TenableADEventsListenerConfiguration.json` y seleccione **Propiedades**.
3. Seleccione la pestaña **Seguridad** y haga clic en **Opciones avanzadas**.
4. Haga clic en la pestaña **Acceso efectivo**.
5. Haga clic en **Seleccionar un usuario**.
6. Escriba `<NOMBRE-DE-CUENTA-DE-SERVICIO-DE-TENABLE>` y haga clic en **Aceptar**.
7. Haga clic en **Ver acceso efectivo**.

8. Compruebe que el permiso “Escribir” esté activo para la cuenta de servicio de Tenable.



Como alternativa, puede usar PowerShell:

- Ejecute los siguientes comandos:

```
Install-Module -Name NTFSSecurity -RequiredVersion 4.2.3
```

```
Get-NTFSEffectiveAccess -Path \\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>\}IOA\ - Account <TENABLE-SERVICE-ACCOUNT-NAME>
```

Para calibrar los loA:

Para evitar ataques falsos positivos o que no se detecten ataques legítimos, tiene que calibrar los loA según el entorno para adaptarlos al tamaño de la instancia de Active Directory, incluir las herramientas conocidas en una whitelist, etc.

1. Consulte [Tenable Identity Exposure Indicators of Attack Reference Guide](#) (Guía de referencia de indicadores de ataque de Tenable Identity Exposure) para obtener información sobre las opciones y los valores recomendados para seleccionar.



2. En el perfil de seguridad, aplique las opciones y los valores a cada loA según se describe en [Personalizar un indicador](#).

Solucionar problemas

Durante la implementación, pueden aparecer los siguientes mensajes de error:

Mensaje	Corrección
"Tenable Identity Exposure no puede escribir en el archivo de configuración porque la carpeta de destino <carpetaDestino> no existe. Esto indica que es posible que haya habido un error en la implementación del módulo de loA".	Desinstale el script y haga clic en "Ver el procedimiento" para obtener instrucciones para volver a instalarlo.
"Tenable Identity Exposure no pudo escribir en el archivo de configuración ubicado en <archivoDestino> para actualizarlo. Esto puede deberse a que otro proceso esté bloqueando el archivo o a cambios de permisos".	<ul style="list-style-type: none">• Asegúrese de que ningún otro proceso, además del módulo de loA, esté usando el archivo de configuración.• Compruebe que la cuenta de servicio tenga permiso para modificar el contenido del archivo.• Si no quiere otorgar permiso a la cuenta de servicio, deshabilite la opción "Actualizaciones automáticas" y haga clic en "Ver el procedimiento" para obtener instrucciones sobre cómo hacer una actualización manual cada vez que modifique la configuración de los loA.
"La carpeta de destino <carpetaDestino> contiene una versión de Tenable Identity Exposure que no puede ejecutar actualizaciones automáticas".	El script instalado actualmente es una versión antigua que usa WMI. Desinstale la versión actual, descargue un nuevo script de instalación y ejecútelo.



“Hubo un error inesperado en la implementación del archivo de configuración”.

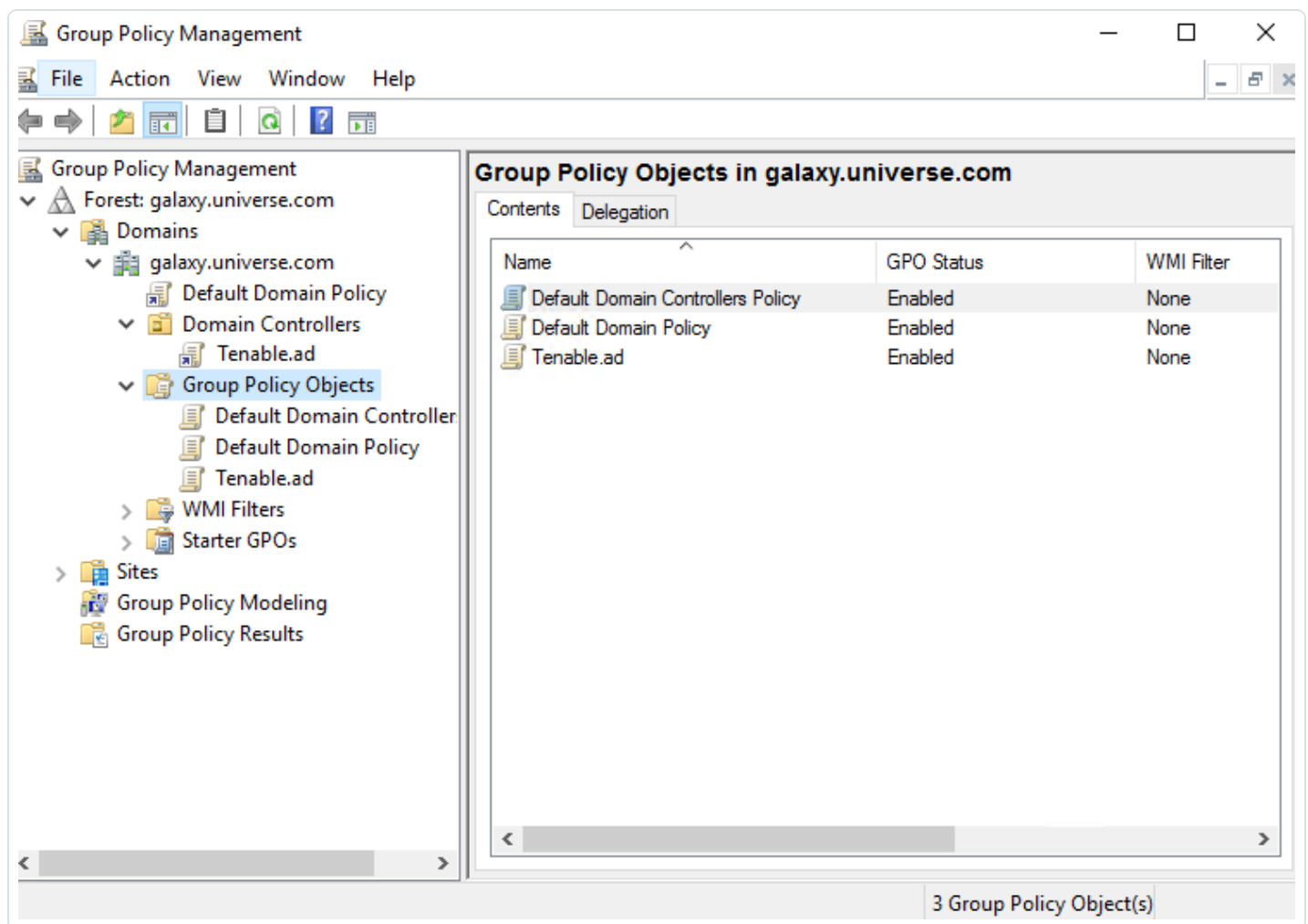
Desinstale el script y haga clic en “Ver el procedimiento” para obtener instrucciones para volver a instalarlo. Si esto no funciona, comuníquese con su representante de atención al cliente.

Para obtener más información, consulte:

- [Script de instalación de indicadores de ataque](#)
- [Cambios técnicos e impacto potencial](#)
- [Detección de antivirus](#)
- [Prioridad de Configuración de directiva de auditoría avanzada](#)

Script de instalación de indicadores de ataque

Después de descargar y ejecutar el archivo de instalación de indicadores de ataque (IoA), el script de IoA crea un nuevo objeto de política de grupo (GPO) llamado de manera predeterminada `Tenable.ad` en la base de datos de Active Directory (AD). El sistema vincula el GPO de Tenable Identity Exposure únicamente a la unidad organizativa (OU) “Controladores de dominio” que contiene todos los controladores de dominio (DC). La nueva política se replica automáticamente entre todos los DC mediante el mecanismo de GPO.



Script de instalación (v. 3.29 y posteriores de Tenable Identity Exposure)

El GPO contiene scripts de PowerShell que todos los DC ejecutan localmente para recopilar datos de interés, de la siguiente manera:

- El script configura un cliente de escucha de registros de eventos en cada controlador de dominio mediante la API EvtSubscribe de Windows. El script establece una suscripción para cada canal de registro de eventos necesario, como se especifica en el archivo de configuración `TenableADEventsListenerConfiguration.json`, para lo que envía una solicitud y una devolución de llamada activada por EvtSubscribe para cada registro de eventos coincidente.
- El cliente de escucha de eventos recibe registros de eventos y los almacena en el búfer antes de vaciarlos periódicamente en un archivo almacenado en un recurso compartido de red



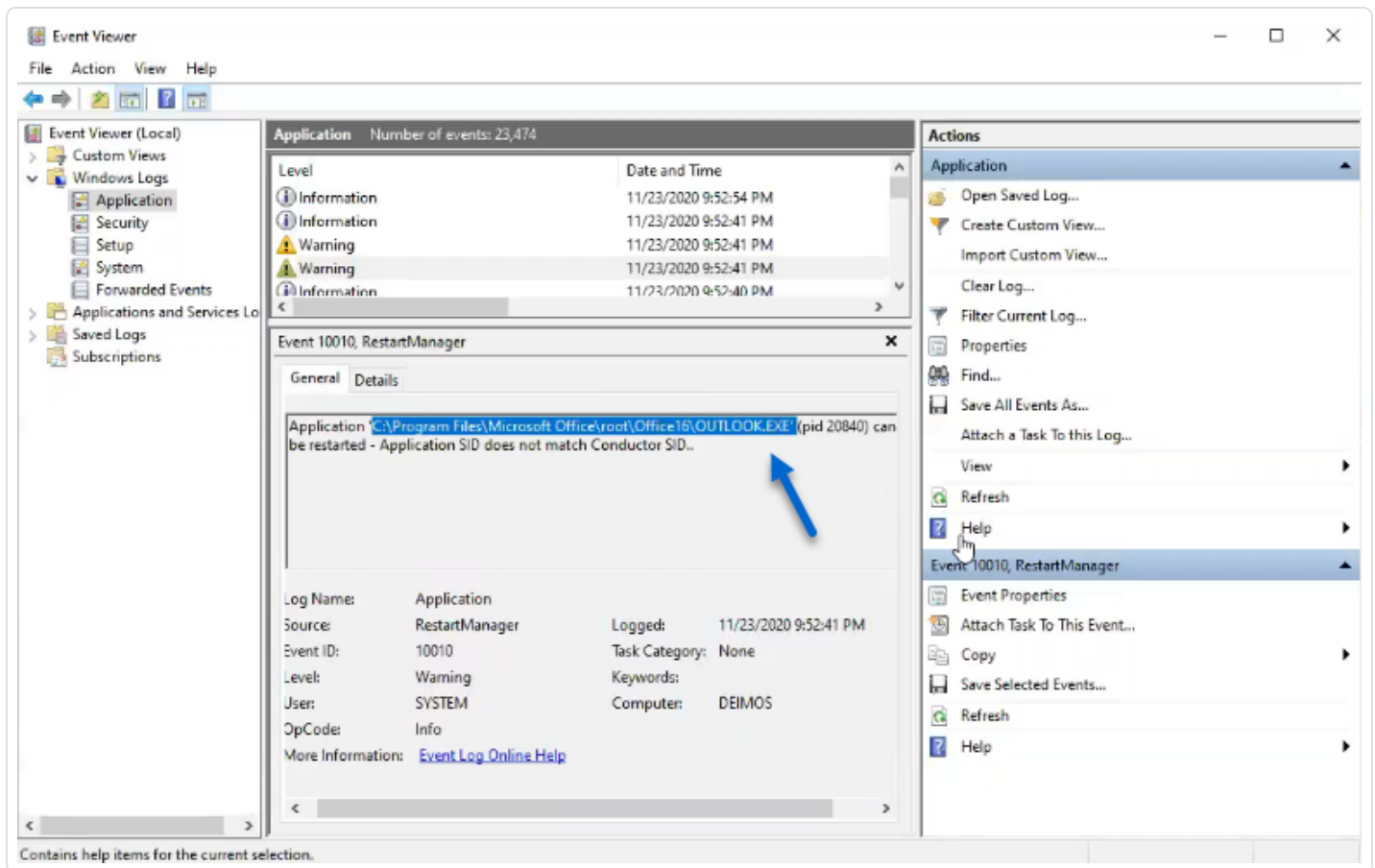
llamado SYSVOL. Cada DC se vacía en un único archivo de SYSVOL que almacena los eventos recopilados y los replica en otros controladores de dominio.

- El script también crea un consumidor de WMI para garantizar que este mecanismo sea persistente al volver a registrar el suscriptor de eventos cuando se reinicia un DC. WMI notifica al consumidor cada vez que se reinicia un DC para permitir que el consumidor registre nuevamente el cliente de escucha de eventos.
- En este momento, se produce la replicación del Sistema de archivos distribuido (DFS) y los archivos se sincronizan automáticamente entre los controladores de dominio. La plataforma de Tenable Identity Exposure escucha el tráfico entrante de replicación de DFS y usa estos datos para recopilar eventos, ejecutar un análisis de seguridad y, luego, generar alertas de loA.

Recuperación de datos locales

Los registros de eventos de Windows registran todos los eventos que tienen lugar en el sistema operativo y sus aplicaciones. Los registros de eventos se basan en un marco de componentes integrados en Windows.

Al usar la API EvtSubscribe, el [cliente de escucha de registros de eventos de loA de Tenable Identity Exposure](#) recopila solo segmentos de datos útiles de los registros de eventos en forma de cadenas de inserción que extrae de los registros de eventos. Tenable Identity Exposure escribe estas cadenas de inserción en un archivo que se almacena en la carpeta SYSVOL y las replica a través del motor de DFS. Esto permite que Tenable Identity Exposure recopile la cantidad justa de datos de seguridad de los registros de eventos para ejecutar un análisis de seguridad y detectar ataques.



Resumen del script de loA

En la siguiente tabla, podrá ver una descripción general de la implementación del script de Tenable Identity Exposure.

Pasos	Descripción	Componente involucrado	Acción técnica
1	Registrar la implementación de loA de Tenable	Gestión de GPO	Crea el GPO Tenable.ad (nombre predeterminado) y lo vincula a la OU "Controladores de dominio".



	Identity Exposure		
2	Iniciar la implementación de loA de Tenable Identity Exposure en DC	Sistema local de DC	Cada DC detecta el nuevo GPO que va a aplicar, según los intervalos de actualización de la política de grupo y de la replicación de AD.
3	Controlar el estado de la política de registro avanzada	Sistema local de DC	El sistema activa la política de registro avanzada mediante la configuración de la clave del registro HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy.
4	Actualizar la política de registro local	Sistema local de DC	Según los loA que se van a detectar, Tenable Identity Exposure genera y activa dinámicamente políticas de auditoría específicas. Esta política no desactiva ninguna política de registro existente; solo las enriquece si es necesario. Si detecta un conflicto, el script de instalación del GPO se detiene y muestra el mensaje "Tenable Identity Exposure requiere la política de auditoría '...', pero la configuración actual de AD impide su uso".
5	Registrar un cliente de escucha de eventos y un productor de WMI	Sistema local de DC	El sistema registra y ejecuta el script incluido en el GPO. Este script ejecuta un proceso de PowerShell para suscribirse a los registros de eventos mediante la API EvtSubscribe y para crear una instancia de ActiveScriptEventConsumer con fines de persistencia. Tenable Identity Exposure usa estos objetos para recibir y almacenar contenido de los registros de eventos.



6	Recopilar mensajes de los registros de eventos	Sistema local de DC	Tenable Identity Exposure captura mensajes pertinentes del registro de eventos, los almacena en el búfer periódicamente y los guarda en archivos (uno por DC) que se almacenan en la carpeta SYSVOL asociada al GPO Tenable Identity Exposure (...{GUID_GPO}\Machine\IOA<nombre_DC>).
7	Replicar archivos en la carpeta SYSVOL del DC declarado	Active Directory	Mediante DFS, AD replica archivos en todo el dominio y, en concreto, en el DC declarado. La plataforma de Tenable Identity Exposure recibe una notificación de cada archivo y lee el contenido.
8	Sobrescribir estos archivos	Active Directory	Cada DC escribe de manera automática y continua en el mismo archivo los eventos almacenados periódicamente en el búfer.

Script de instalación (v. 3.19.11 y anteriores de Tenable Identity Exposure)

El GPO contiene scripts de PowerShell que todos los DC ejecutan localmente para recopilar datos de interés, de la siguiente manera:

- Los scripts configuran un observador de eventos y un productor o consumidor de Instrumental de administración de Windows (WMI) en la memoria de la máquina. WMI es un componente de Windows que le brinda información sobre el estado de los sistemas informáticos locales o remotos.
- El observador de eventos recibe registros de eventos y los almacena periódicamente en el búfer antes de vaciarlos en un archivo almacenado en un recurso compartido de red llamado SYSVOL. Cada DC se vacía en un único archivo de SYSVOL que almacena los eventos recopilados y los replica en otros controladores de dominio.
- El consumidor de WMI hace que este mecanismo sea persistente al registrar nuevamente el observador de eventos cuando se reinicia un DC. El productor se activa y notifica al consumidor cada vez que se reinicia un DC. Como consecuencia, el consumidor vuelve a



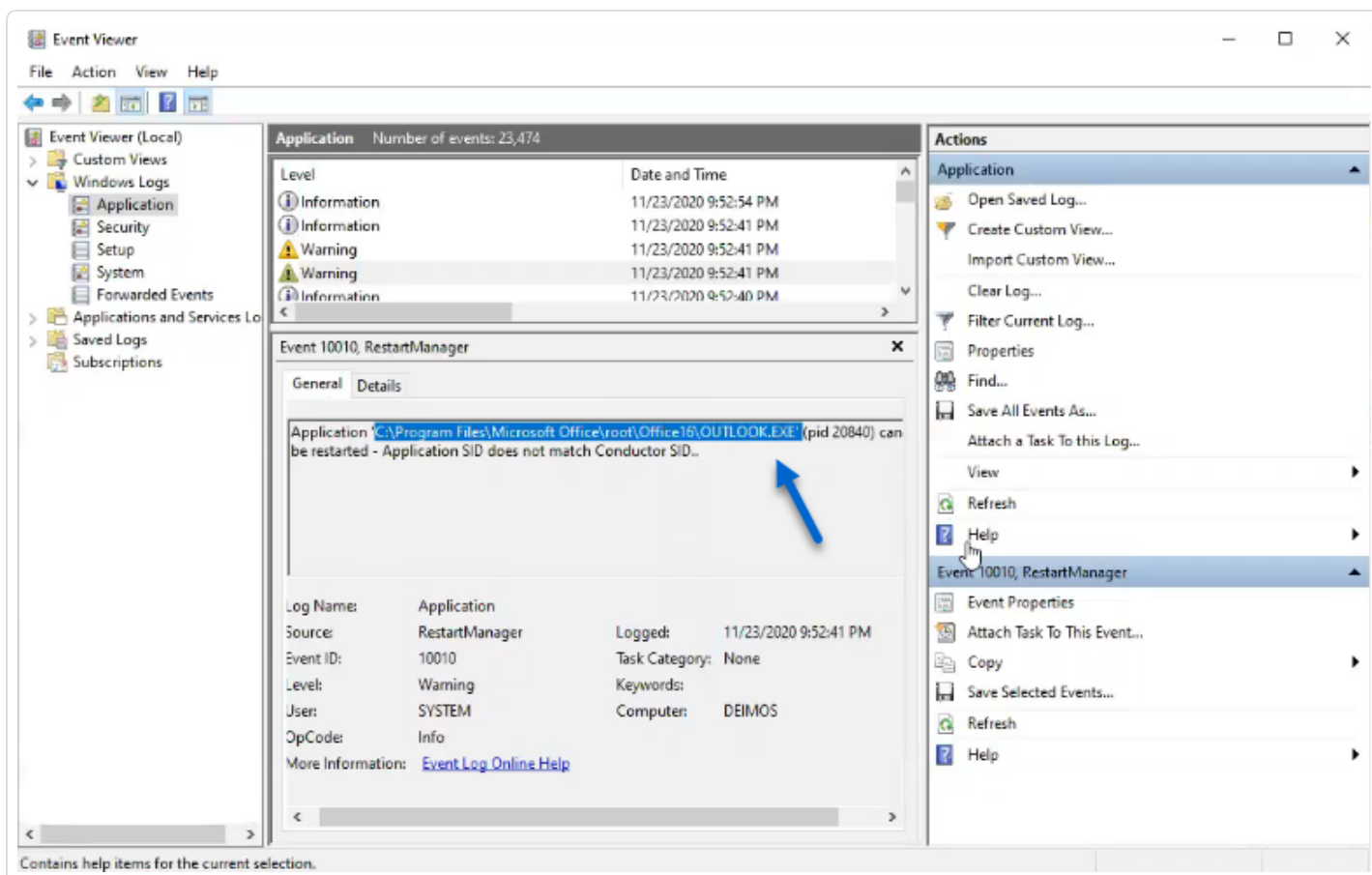
registrar el observador de eventos.

- En este momento, se produce la replicación del Sistema de archivos distribuido o DFS y los archivos se sincronizan automáticamente entre los controladores de dominio. La plataforma de Tenable Identity Exposure escucha el tráfico entrante de replicación de DFS y usa estos datos para recopilar eventos, ejecutar un análisis de seguridad y, luego, generar alertas de IoA.

Recuperación de datos locales

Los registros de eventos de Windows registran todos los eventos que tienen lugar en el sistema operativo y sus aplicaciones. Los registros de eventos llamados Seguimiento de eventos para Windows (ETW) se basan en un marco de componentes integrados en Windows. ETW se encuentra en el kernel y produce datos que se almacenan localmente en los DC y que los protocolos de AD no replican.

Al usar el motor de WMI, Tenable Identity Exposure recopila solo segmentos de datos útiles de ETW en forma de cadenas de inserción que extrae de los registros de eventos. Tenable Identity Exposure escribe estas cadenas de inserción en un archivo que se almacena en la carpeta SYSVOL y las replica a través del motor de DFS. Esto permite que Tenable Identity Exposure recopile la cantidad justa de datos de seguridad de ETW para ejecutar un análisis de seguridad y detectar ataques.



Resumen del script de loA

En la siguiente tabla, podrá ver una descripción general de la implementación del script de Tenable Identity Exposure.

Pasos	Descripción	Componente involucrado	Acción técnica
1	Registrar la implementación de loA de Tenable	Gestión de GPO	Crea el GPO Tenable.ad (nombre predeterminado) y lo vincula a la OU "Controladores de dominio".



	Identity Exposure		
2	Iniciar la implementación de loA de Tenable Identity Exposure en DC	Sistema local de DC	Cada DC detecta el nuevo GPO que va a aplicar, según los intervalos de actualización de la política de grupo y de la replicación de AD.
3	Registrar un observador de eventos y un productor o consumidor de WMI	Sistema local de DC	El sistema registra y ejecuta una tarea inmediata. Esta tarea ejecuta un proceso de PowerShell para crear instancias de las siguientes clases: ManagementEventWatcher y ActiveScriptEventConsumer. Tenable Identity Exposure usa estos objetos para recibir y almacenar mensajes de ETW.
4	Controlar el estado de la política de registro avanzada	Sistema local de DC	El sistema activa la política de registro avanzada mediante la configuración de la clave del registro HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy.
5	Actualizar la política de registro local	Sistema local de DC	Según los loA que se van a detectar, Tenable Identity Exposure genera y activa dinámicamente una política de registro avanzada. Esta política no desactiva ninguna política de registro existente; solo las enriquece si es necesario. Si detecta un conflicto, el script de instalación del GPO se detiene y muestra el mensaje "Tenable Identity Exposure requiere la política de auditoría '...', pero la



			configuración actual de AD impide su uso”.
6	Recopilar mensajes de ETW	Sistema local de DC	Tenable Identity Exposure captura mensajes de ETW pertinentes, los almacena en el búfer periódicamente y los guarda en archivos (uno por DC) que se almacenan en la carpeta SYSVOL asociada al GPO Tenable Identity Exposure (...{GUID_GPO}\Machine\IOA<nombre_DC>).
7	Replicar archivos en la plataforma de Tenable Identity Exposure	Active Directory	Mediante DFS, AD replica archivos en todo el dominio. La plataforma de Tenable Identity Exposure también recibe los archivos.
8	Sobrescribir estos archivos	Active Directory	Cada DC escribe de manera automática y continua en el mismo archivo los eventos almacenados periódicamente en el búfer.

Consulte también

- [Instalar indicadores de ataque](#)
- [Cambios técnicos e impacto potencial](#)

Cambios técnicos e impacto potencial

El script de instalación del módulo de indicadores de ataque (IoA) crea un GPO que aplica los siguientes cambios de forma transparente en los DC supervisados:

- Un nuevo GPO denominado “Tenable.ad” vinculado de manera predeterminada a la unidad organizativa (OU) “Controladores de dominio”.
- Modificación de una clave del registro para activar la política de registro avanzada de Microsoft.



- Activación de una nueva política de registro de eventos para obligar a los controladores de dominio a generar la información de ETW que requieren los loA.

Nota: La política de registro de eventos es obligatoria para que el motor de ETW pueda generar las cadenas de inserción que Tenable Identity Exposure requiere. Esta política no deshabilita ninguna política de registro existente, sino que las complementa. Si hay un conflicto, el script de implementación se detiene con un mensaje de error.

- Adición de un permiso de escritura para la cuenta de servicio de Tenable Identity Exposure que permite "Actualizaciones automáticas" de la configuración de loA almacenada en la carpeta de GPO.

Limitaciones e impacto potencial

El módulo de **indicadores de ataque** (loA) puede presentar las siguientes limitaciones:

- El módulo de loA se basa en los datos de ETW y funciona dentro de las limitaciones que define Microsoft.
- El GPO instalado debe replicarse en todo el dominio, y el intervalo de actualización del GPO debe transcurrir para que se complete el proceso de instalación. Durante este período de replicación, pueden producirse falsos positivos y falsos negativos, aunque Tenable Identity Exposure minimiza este efecto al no iniciar inmediatamente las verificaciones en el motor de indicadores de ataque.
- Tenable usa el recurso compartido de archivos de SYSVOL para recuperar información de ETW de los controladores de dominio. A medida que SYSVOL se replica en cada controlador de dominio del dominio, aparece un aumento significativo de la actividad de replicación durante un pico alto de actividad de Active Directory.
- La replicación de archivos entre controladores de dominio y Tenable Identity Exposure también consume parte del ancho de banda de red. Para controlar estos efectos, Tenable Identity Exposure elimina automáticamente los archivos que recopila y limita el tamaño de estos archivos (valor predeterminado de 500 MB como máximo).
- Problemas con la replicación lenta o interrumpida del Sistema de archivos distribuido (DFS). Para obtener más información, consulte [Mitigación de problemas de replicación de DFS](#).

Consulte también



- [Indicators of Attack and the Active Directory](#)
- [Instalar indicadores de ataque](#)
- [Script de instalación de indicadores de ataque](#)
- [Solucionar problemas de indicadores de ataque](#)

Escenarios de ataque (< v. 3.36)

Precaución: Esta funcionalidad de actualización de la configuración de los indicadores de ataque ya no se aplica a las versiones de Tenable Identity Exposure posteriores a la 3.36.

Rol de usuario obligatorio: usuario de la organización con permisos para modificar la configuración de los indicadores de ataque.

Para definir un escenario de ataque, seleccione los tipos de ataque que quiere que Tenable Identity Exposure supervise en dominios específicos.

Antes de empezar

Para modificar el escenario de ataque, debe tener un rol de usuario con los siguientes permisos:

- En **Entidades de datos**, acceso “Leer” para:
 - Todos los indicadores de ataque
 - Todos los dominios
- En **Entidades de interfaz**, acceso para:
 - Gestión > Sistema > Configuración
 - Gestión > Sistema > Configuración > Servicios de aplicación > Indicadores de ataque
 - Gestión > Sistema > Configuración > Servicios de aplicación > Indicadores de ataque > Descargar archivo de instalación

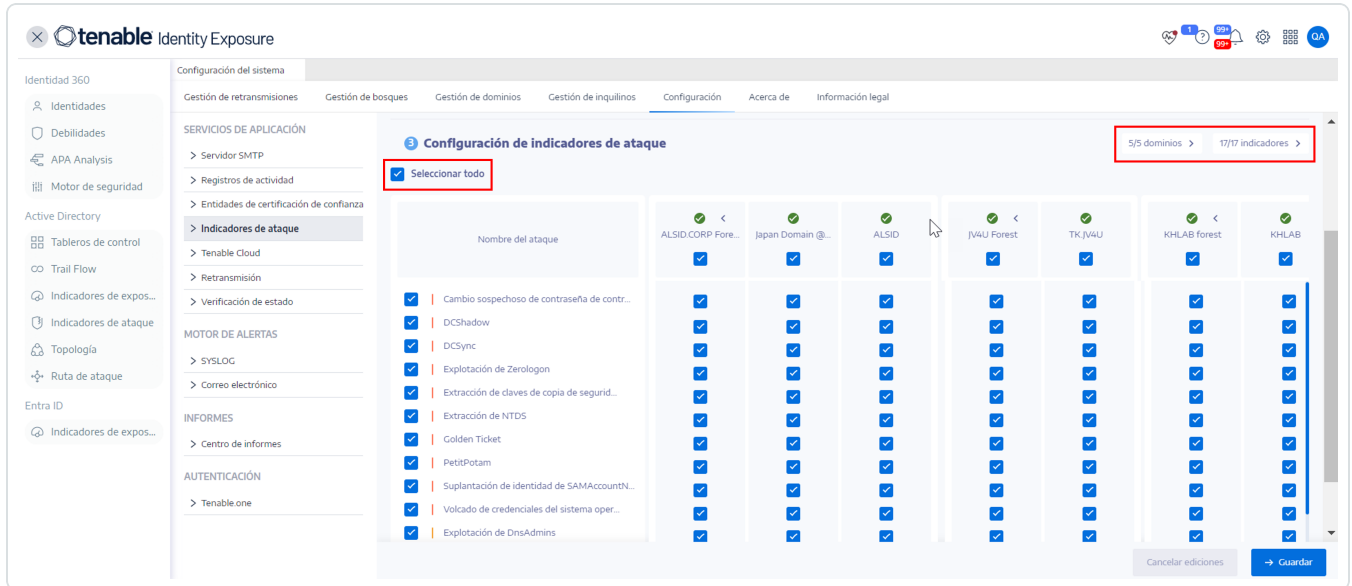
Para obtener más información sobre los permisos basados en roles, consulte [Establecer permisos para un rol](#).

Para definir un escenario de ataque:



1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración > Indicadores de ataque**.

Se abre el panel **Definición de escenarios de ataque**.



2. En **Nombre del ataque**, seleccione el ataque que quiere supervisar.

3. Seleccione el dominio que quiere supervisar para detectar el ataque seleccionado.

4. De manera opcional, puede seguir uno de los procedimientos a continuación:

- Hacer clic en **Seleccionar todo** para supervisar todos los ataques en todos los dominios.
- Hacer clic en **n/n dominios** o **n/n indicadores** para filtrar dominios específicos y supervisar ataques específicos.

5. Haga clic en **Guardar**.

Un mensaje de confirmación le informa que Tenable Identity Exposure borra el estado de actividad de cada ataque después guardar la configuración.

6. Haga clic en **Confirmar**.

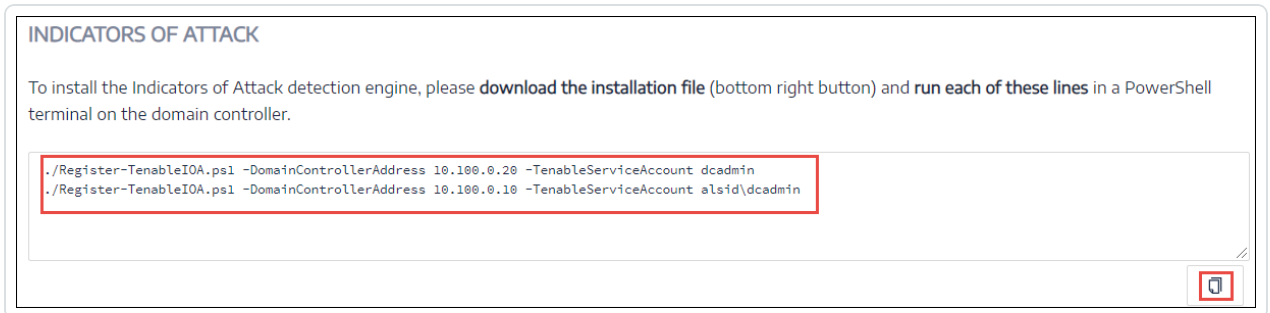
Un mensaje confirma que Tenable Identity Exposure actualizó la configuración de los indicadores de ataque.

7. Haga clic en **Descargar el archivo de instalación**.

8. Para que la nueva configuración de ataque surta efecto, ejecute el archivo de instalación:



- a. Copie el archivo de instalación descargado y péguelo en el controlador de dominio del dominio supervisado.
- b. Abra un terminal de PowerShell con derechos administrativos.
- c. En Tenable Identity Exposure, copie los comandos debajo de la sección “Indicadores de ataque” al final de la ventana.



- d. En la ventana de PowerShell, pegue los comandos para ejecutar el script.

Cuota de carga de trabajo

Precaución: La funcionalidad de cuota de carga de trabajo ya no se aplica únicamente a las versiones de Tenable Identity Exposure posteriores a la 3.36.

Rol de usuario obligatorio: usuario de la organización con permisos para editar la cuota de carga de trabajo.

Cada indicador de ataque en Tenable Identity Exposure tiene una cuota de carga de trabajo asociada que tiene en cuenta los recursos necesarios para analizar los datos de un ataque.

Tenable Identity Exposure calcula la cuota de carga de trabajo para limitar la cantidad de indicadores de ataque (IoA) que se ejecutan simultáneamente, lo que tiene un efecto en el ancho de banda y en el uso de la CPU para la generación de eventos en los controladores de dominio.

Después de modificar el límite de la cuota de carga de trabajo, haga lo siguiente:

- Aumento: supervise las estadísticas tras el aumento para garantizar un margen cómodo.
- Disminución: desactive algunos IoA para permanecer por debajo de esta cuota, lo que reduce la cobertura de seguridad contra ataques.

Para modificar el límite de la cuota de carga de trabajo:



1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración > Indicadores de ataque**.
Se abre el panel **Configuración de loA**.
2. Seleccione los loA que quiere para su configuración.
3. En **Indicadores de ataque**, en el cuadro **Límite máximo de cuota**, escriba un valor para el límite de cuota de carga de trabajo.

Attack name	Workload Quota	Forest1	alsid	Forest2	tenable
<input checked="" type="checkbox"/> Password Guessing	...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Password Spraying	...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Enumeration of local administrators	...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Massive computers reconnaissance	...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Kerberoasting	...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> NTDS Extraction	...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

INDICATORS OF ATTACK
Quota maximum limit: 75 Workload Quota used: 59 / 75

4. Haga clic en la marca de verificación junto al valor que ingresó.

Un mensaje le informa sobre el efecto de la modificación en Tenable Identity Exposure.

Nota: Si escribe un límite máximo de cuota que sea menor que el que exige la configuración de ataque actual, tendrá que ajustar la cantidad de indicadores de ataque activos o aumentar el límite.

5. Haga clic en **Confirmar**.

Un mensaje confirma que Tenable Identity Exposure actualizó el límite máximo de la cuota.

6. Haga clic en **Guardar**.

Un mensaje de confirmación le informa que Tenable Identity Exposure borra el estado de actividad de cada ataque después guardar la configuración.



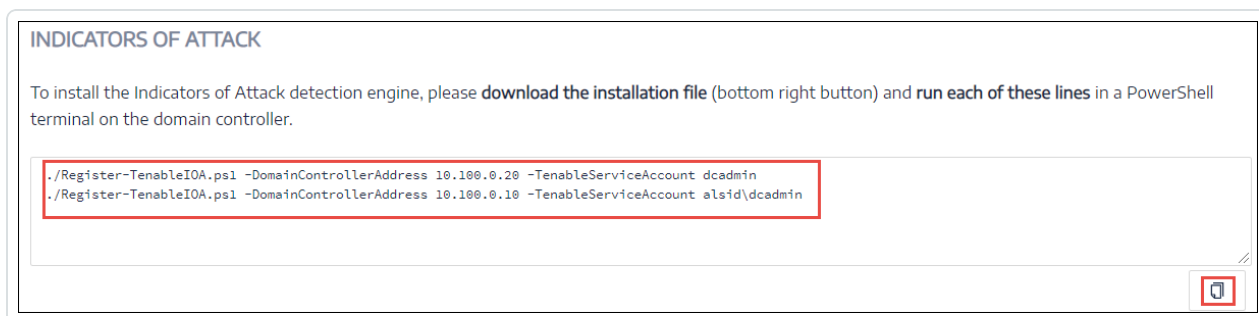
7. Haga clic en **Confirmar**.

Un mensaje confirma que Tenable Identity Exposure actualizó la configuración de los indicadores de ataque.

8. Haga clic en **Descargar el archivo de instalación**.

9. Para que la nueva configuración de ataque surta efecto, ejecute el archivo de instalación:

- a. Copie el archivo de instalación descargado y péguelo en el controlador de dominio del dominio supervisado.
- b. Abra un terminal de PowerShell con derechos administrativos.
- c. En Tenable Identity Exposure, copie los comandos debajo de la sección "Indicadores de ataque" al final de la ventana.



d. En la ventana de PowerShell, pegue los comandos para ejecutar el script.

Instalar Microsoft Sysmon

Algunos indicadores de ataque (IoA) de Tenable Identity Exposure requieren que se active el servicio System Monitor (Sysmon) de Microsoft.

Sysmon supervisa y registra la actividad del sistema en el registro de eventos de Windows para proporcionar más información orientada a la seguridad en la infraestructura de Seguimiento de eventos para Windows (ETW).

Dado que instalar un servicio y un controlador de Windows adicionales puede afectar el rendimiento de los controladores de dominio que hospedan la infraestructura de Active Directory, Tenable no implementa automáticamente Microsoft Sysmon. Debe instalarlo manualmente o usar un GPO dedicado.



Los siguientes loA requieren Microsoft Sysmon.

Nombre	Motivo
Volcado de credenciales del sistema operativo: memoria de LSASS	Detecta la inyección de procesos.

Nota: Si elige instalar Sysmon, debe instalarlo en todos los controladores de dominio y no solo en el PDC para recopilar todos los eventos necesarios.

Nota: Pruebe la instalación de Sysmon para detectar problemas de compatibilidad antes de realizar una implementación completa de Tenable Identity Exposure.

Sugerencia: Asegúrese de actualizar Sysmon periódicamente después de la instalación para aprovechar los parches que aborden posibles vulnerabilidades. La versión más antigua compatible con Tenable Identity Exposure es Sysmon 12.0.

Para instalar Sysmon:

1. Descargue Sysmon del sitio web de Microsoft.
2. En la interfaz de la línea de comandos, ejecute el siguiente comando para instalar Microsoft Sysmon en la máquina local:

```
.\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
```

Nota: Consulte el [archivo de configuración de Sysmon](#) comentado para obtener explicaciones sobre la configuración.

3. Ejecute el siguiente comando para agregar una clave del registro para indicar a los filtros de WMI que Sysmon está instalado:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon\Operational"
```

Para desinstalar Sysmon:



1. Abra un terminal de PowerShell.
2. Busque la carpeta que contiene Sysmon64.exe.
3. Escriba el siguiente comando:

```
PS C:\> .\Sysmon64.exe -u
```

Para eliminar la clave del registro:

- En la interfaz de la línea de comandos, escriba el siguiente comando en todas las máquinas que ejecutan Sysmon:

```
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon\Operational"
```

Archivo de configuración de Sysmon

Notas:

- Copie el archivo de configuración de Sysmon y guárdelo como archivo XML antes de usarlo. En caso de error, también puede descargar el archivo de configuración directamente [aquí](#).
- Desbloquee el archivo en las propiedades del archivo antes de ejecutarlo.

```
<Sysmon schemaversion="4.40">
  <EventFiltering>

    <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM
[FileCreateTime]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateTime onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateTime>
    </RuleGroup>

    <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </NetworkConnect>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```



```
</NetworkConnect>
</RuleGroup>

<!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
  <!--Cannot be filtered.-->

<!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
<RuleGroup name="" groupRelation="or">
  <ProcessTerminate onmatch="exclude">
    <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
  </ProcessTerminate>
</RuleGroup>

<!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
<RuleGroup name="" groupRelation="or">
  <DriverLoad onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </DriverLoad>
</RuleGroup>

<!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
<RuleGroup name="" groupRelation="or">
  <ImageLoad onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </ImageLoad>
</RuleGroup>

<!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
<RuleGroup name="" groupRelation="or">
  <CreateRemoteThread onmatch="include">
    <TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  </CreateRemoteThread>
</RuleGroup>

<!--SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
<RuleGroup name="" groupRelation="or">
  <RawAccessRead onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </RawAccessRead>
</RuleGroup>

<!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
<RuleGroup name="" groupRelation="or">
  <ProcessAccess onmatch="include">
    <!-- Detect Access to LSASS-->
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1FFFFFF</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1F1FFF</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
```



```
<GrantedAccess>0x1010</GrantedAccess>
</Rule>
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x143A</GrantedAccess>
</Rule>

<!-- Detect process hollowing to LSASS-->
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x0800</GrantedAccess>
</Rule>
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x800</GrantedAccess>
</Rule>

<!-- Detect process process injection to LSASS-->
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x0820</GrantedAccess>
</Rule>
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x820</GrantedAccess>
</Rule>
</ProcessAccess>
</RuleGroup>

<!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
<RuleGroup name="" groupRelation="or">
  <FileCreate onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </FileCreate>
</RuleGroup>

<!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->
<RuleGroup name="" groupRelation="or">
  <RegistryEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </RegistryEvent>
</RuleGroup>

<!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->
<RuleGroup name="" groupRelation="or">
  <FileCreateStreamHash onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </FileCreateStreamHash>
</RuleGroup>

<!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
<!--Cannot be filtered.-->
```



```
<!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->
<RuleGroup name="" groupRelation="or">
  <PipeEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </PipeEvent>
</RuleGroup>

<!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
<RuleGroup name="" groupRelation="or">
  <WmiEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </WmiEvent>
</RuleGroup>

<!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
<RuleGroup name="" groupRelation="or">
  <DnsQuery onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </DnsQuery>
</RuleGroup>

<!--SYSMON EVENT ID 23 : FILE DELETED [FileDelete]-->
<RuleGroup name="" groupRelation="or">
  <FileDelete onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </FileDelete>
</RuleGroup>

</EventFiltering>
</Sysmon>
```

Desinstalar indicadores de ataque

Rol obligatorio: administrador en la máquina local.

Para desinstalar el módulo de indicadores de ataque (IoA), ejecute un comando que cree un nuevo objeto de política de grupo (GPO) llamado "Tenable Identity Exposure cleaning".

El proceso de desinstalación usa este nuevo GPO de manera predeterminada para limpiar los GPO previamente instalados y sus archivos de SYSVOL, la configuración del registro, la política de registro avanzada y los filtros de WMI.

Nota: Si cambió el nombre del GPO inicial, debe pasárselo al desinstalador para que sepa qué GPO tiene que desinstalar. Para pasar el nuevo nombre del GPO, use el parámetro `-GpoDisplayName`.

Para desinstalar el módulo de IoA:



1. En la interfaz de la línea de comandos, ejecute el siguiente comando para desinstalar el módulo de loA:

```
Register-TenableIOA.ps1 -Uninstall
```

2. Replique este nuevo GPO en todo el dominio. El script impone un retraso de 4 horas para que se complete la replicación.
3. Ejecute el siguiente comando para eliminar el GPO "cleaning":

```
Remove-GPO -Guid <GUID> -Domain "<DOMAIN>"
```

4. Opcional: Ejecute el siguiente comando para verificar que el GPO ya no exista:

```
(Get-ADDomainController -Filter *).Name | Foreach-Object {Get-GPO -Name "Tenable.ad cleaning"}  
| Select Displayname| measure
```

Ahora desinstaló los loA por completo. Sin embargo, las entradas del registro pueden persistir si otro GPO no las define. A continuación se muestran las entradas del registro que utilizó el loA "Reconocimiento masivo de equipos" (pueden variar según la configuración específica del loA):

- HKLM\MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\AuditReceivingNTLMTraffic (valor: 2)
- HKLM\MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\RestrictSendingNTLMTraffic (valor: 1)
- HKLM\MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\AuditNTLMInDomain (valor: 7)

Para eliminar estas entradas del registro, ejecute el siguiente script de PowerShell en todos los controladores de dominio:

```
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa\MSV1_0" -Name  
"AuditReceivingNTLMTraffic"  
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa\MSV1_0" -Name  
"RestrictSendingNTLMTraffic"  
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Services\Netlogon\Parameters" -Name  
"AuditNTLMInDomain"
```

Eliminación manual de carpetas de GPO obsoletas de SYSVOL



En algunos casos, al reinstalar el GPO de loA, es posible que las carpetas más antiguas permanezcan en el directorio de SYSVOL debido a una característica de Microsoft. Si Directory Listener reconoce estas carpetas obsoletas como la carpeta de loA, puede provocar errores de detección.

Siga el procedimiento a continuación para garantizar una eliminación limpia de las carpetas de GPO de loA obsoletas y evitar problemas de detección durante la reinstalación.


Para eliminar carpetas de GPO de loA obsoletas:

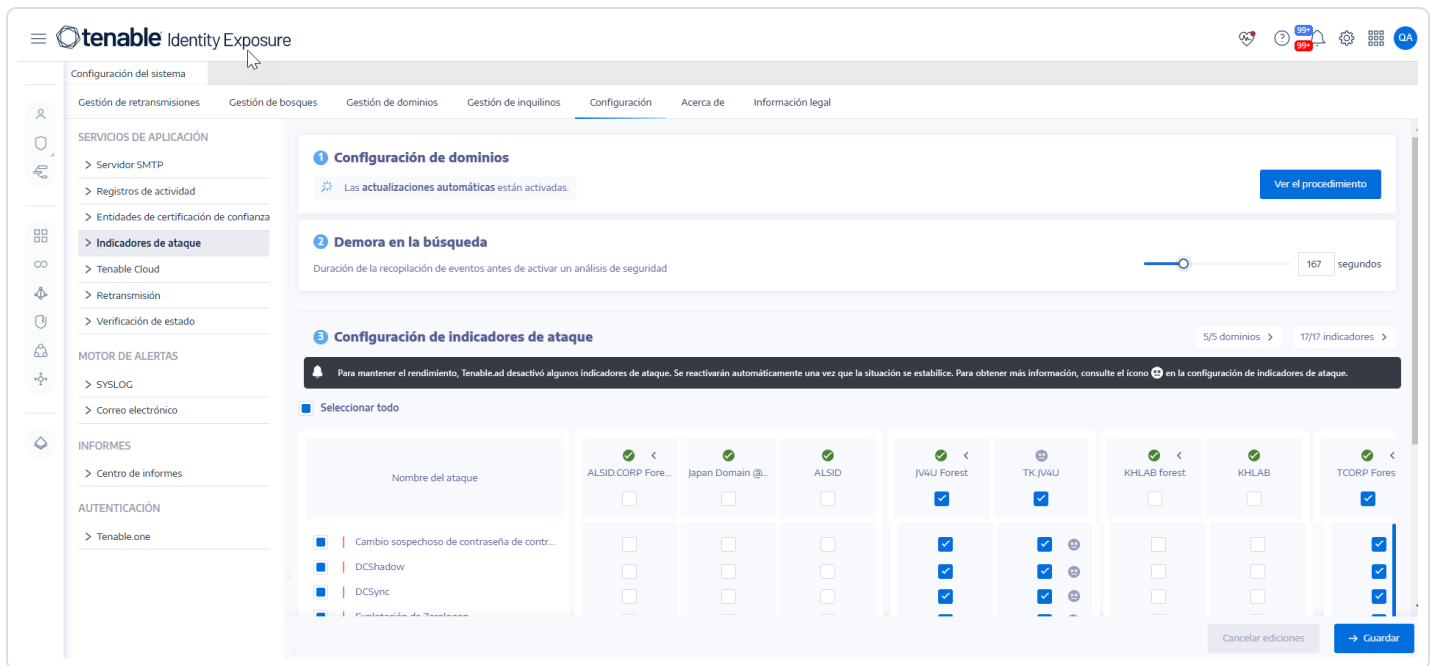
Elimine manualmente las carpetas de loA obsoletas del directorio de SYSVOL que no correspondan al GUID del GPO de loA más reciente. Asegurarse de que solo permanezca el objeto de política de grupo (GPO) más actualizado mantiene la coherencia y evita posibles conflictos entre las políticas.

Si necesita más orientación o tiene algún problema, comuníquese con el equipo de soporte para obtener asistencia.

Indicadores de ataque desactivados



En ocasiones, puede que Tenable Identity Exposure desactive temporalmente algunos indicadores de ataque (loA) para mantener un rendimiento óptimo.

Cuando un loA está desactivado, se muestra el ícono  a un lado.




Íconos de estado de los loA

Íconos de estado de la primera fila



- Ícono gris : indica que al menos un loA está desactivado temporalmente.
- Ícono de marca de verificación verde : indica que todos los loA configurados están activados.

Íconos de estado de las otras filas


- Ícono gris : aparece junto a dominios específicos donde los loA están desactivados.

Información sobre herramientas

Al pasar el cursor sobre los íconos de estado, verá la siguiente información sobre herramientas:

- Ícono gris : "Uno o varios indicadores de ataque se desactivaron temporalmente".
- Ícono de marca de verificación verde : "Todos los loA configurados están activados".



- Ícono gris  en otras filas: “El indicador de ataque se desactivó temporalmente (desde yyyy-mm-dd hh:mm) para mantener el rendimiento”.

Mensaje de alerta

Cuando Tenable Identity Exposure desactiva algún loA, aparece un mensaje de alerta encima de la tabla de loA:

“Para mantener el rendimiento, Tenable Identity Exposure desactivó algunos loA. Se reactivarán automáticamente una vez que la situación se estabilice. Para obtener más información, consulte el ícono en la configuración de indicadores de ataque”.

Reglas de visibilidad

El estado desactivado es visible tanto en el nivel de dominio como de bosque.

- Si desmarca un dominio con un ícono de desactivación y ningún otro dominio tiene este ícono, desaparece del dominio vinculado.
- Si todos los dominios vinculados a un bosque ya no tienen íconos de desactivación, el ícono desaparece del bosque vinculado.

Reactivación automática

Tenable Identity Exposure reactiva automáticamente los loA desactivados una vez que el rendimiento del sistema se estabiliza. No se requiere intervención manual.

La desactivación temporal de los loA es una funcionalidad integrada diseñada para mantener el rendimiento del sistema. Tenable Identity Exposure ajusta dinámicamente los loA activos para garantizar un funcionamiento óptimo sin poner en peligro las funcionalidades de supervisión de la seguridad.

Responder al ícono gris de “desactivado”

Cuando aparezca el ícono gris de “desactivado”:

1. Espere a que la situación se resuelva: en la mayoría de los casos, lo único que tiene que hacer es esperar. Tenable Identity Exposure reactiva automáticamente los loA una vez que el



rendimiento del sistema se estabiliza.

2. Para implementaciones locales:

- Si observa que esto sucede con frecuencia, a pesar de seguir las recomendaciones de la matriz de recursos, es posible que tenga que agregar más recursos a la máquina que aloja el servicio Cygni.
- Considere la posibilidad de actualizar la CPU, la RAM o el espacio en disco según sea necesario para mejorar el rendimiento general del sistema.

3. Supervise la frecuencia: haga un seguimiento de la frecuencia con la que aparece este ícono. Si aparece a menudo, puede indicar que los recursos actuales están constantemente bajo presión.

4. Revise la configuración de los loA: mientras espera la reactivación, es posible que quiera revisar la configuración actual de los loA para asegurarse de que se alinee con sus necesidades de seguridad y los recursos disponibles.

Solucionar problemas de indicadores de ataque

- [Prioridad de Configuración de directiva de auditoría avanzada](#)
- [Detección de antivirus](#)
- [Archivos de registros de Tenable Identity Exposure](#)
- [Validación del cliente de escucha de registros de eventos](#)
- [Mitigación de problemas de replicación de DFS](#)
- [Retención de registros de eventos de Windows](#)
- [Entradas "desconocidas" en las alertas de indicadores de ataque](#)
- [Indicadores de ataque operativos](#)

Detección de antivirus

Tenable y Microsoft no recomiendan instalar software antivirus, de plataformas de protección de puntos de conexión (EPP) ni de detección y respuesta de puntos de conexión (EDR) en los controladores de dominio (ni en ninguna otra herramienta con una consola de administración central). Si decide hacerlo, es posible que el antivirus, EPP o EDR detecten e, incluso, bloqueen o



eliminen elementos necesarios para la recopilación de eventos de los indicadores de ataque (IoA) en los controladores de dominio.

El script de implementación de Tenable Identity Exposure para los indicadores de ataque no incluye código malintencionado y ni siquiera está ofuscado. Sin embargo, las detecciones ocasionales son normales, dado el uso de PowerShell y WMI y la naturaleza sin agente de la implementación.

Si encuentra problemas como los siguientes:

- Mensajes de error durante la instalación
- Falsos positivos o falsos negativos en la detección

Para solucionar problemas de detección de antivirus en scripts de instalación:

1. Revise los registros de seguridad del antivirus, EPP o EDR para comprobar si se detectaron, bloquearon o eliminaron componentes de Tenable Identity Exposure. El antivirus, EPP o EDR pueden afectar los siguientes componentes:
 - El archivo `ScheduledTasks.xml` en el GPO de Tenable Identity Exposure que se aplicó en los controladores de dominio.
 - La tarea programada de Tenable Identity Exposure en los controladores de dominio que inicia `PowerShell.exe`.
 - El proceso `Register-TenableADEventsListener.exe` de Tenable Identity Exposure que se inició en los controladores de dominio.
2. Agregue excepciones de seguridad a las herramientas para los componentes afectados.
 - En particular, Symantec Endpoint Protection puede generar detecciones de `CL.Downloader!gen27` durante el proceso de instalación de los IoA. Puede agregar este riesgo conocido específico a su política de excepciones.
 - Una vez que haya configurado el Programador de tareas, ejecute PowerShell para iniciar el proceso `Register-TenableADEventsListener.exe`. El software antivirus, EPP o EDR tiene el potencial de obstruir este script de PowerShell, lo que dificulta la correcta ejecución de los indicadores de ataque. Haga un seguimiento minucioso de este proceso y asegúrese de que se ejecute solo una vez en todos los controladores de



dominio supervisados.

Ejemplos de exclusiones de rutas de archivos para antivirus, EPP o EDR:

```
Register-TenableADEventsListener.exe process  
"\\\"domain\"\\sysvol\"domain\"\\Policies\"{\"GUID_Tenable.ad\"}\\Machine\\IOA\\Register-  
TenableADEventsListener.exe"
```

```
ScheduledTasks.xml file  
C:\\Users\\<User Name>\\AppData\\Local\\Temp\\4\\Tenable.ad\\  
{GUID}\\DomainSysvol\\GPO\\Machine\\Preferences\\ScheduledTasks\\ScheduledTasks.xml  
C:\\Windows\\[SYSVOL]\\POLICIES\\  
{[GUID]}\\Machine\\Preferences\\ScheduledTasks\\ScheduledTasks.xml  
  \\[DOMAIN.FQDN]\\[SYSVOL]\\POLICIES\\  
{[GUID]}\\Machine\\Preferences\\ScheduledTasks\\ScheduledTasks.xml
```

Prioridad de Configuración de directiva de auditoría avanzada

El objeto de política de grupo (GPO) que Tenable Identity Exposure crea para habilitar el registro de eventos necesarios está vinculado a los controladores de dominio de la unidad organizativa (OU) con el modo Forzado habilitado.

Esto le otorga al GPO una prioridad alta, pero un GPO forzado configurado en un nivel superior (como un dominio o sitio) tiene prioridad sobre él.

Si el GPO de mayor prioridad que define las opciones de Configuración de directiva de auditoría avanzada entra en conflicto con las necesidades de Tenable Identity Exposure, tiene prioridad y Tenable Identity Exposure omite los eventos necesarios para la detección de ataques.

Dado que Windows fusiona las opciones de Configuración de directiva de auditoría avanzada definidas por los GPO, distintos GPO pueden definir opciones diferentes.

Sin embargo, para cada opción, solo usa el valor definido por el GPO con mayor precedencia. Por ejemplo, Tenable Identity Exposure necesita el valor Correcto y Error para la opción Auditar validación de credenciales. Sin embargo, si un GPO con mayor precedencia solo define Correcto para Auditar validación de credenciales, Windows solo recopila eventos con Correcto y Tenable Identity Exposure omite los eventos con Error necesarios.

Para comprobar la precedencia de los GPO:



1. En la interfaz de la línea de comandos, ejecute el siguiente comando en un controlador de dominio.

Genera la Configuración de directiva de auditoría avanzada vigente después de tener en cuenta todos los GPO y la precedencia.

```
auditpol.exe /get /category:*
```

2. Compare la salida con los requisitos de las políticas de auditoría avanzada de Tenable Identity Exposure. Para cada opción que Tenable Identity Exposure exija, verifique que la política vigente también la cubra.
 - No es problema si la política vigente es más exhaustiva, como cuando Tenable Identity Exposure necesita "Correcto" o "Error" y la opción es "Correcto y error".
 - Si la política vigente es insuficiente, se debe a que un GPO con mayor precedencia define opciones en conflicto.

Para corregir la precedencia de los GPO:

1. Busque los GPO vinculados a niveles superiores (dominio o sitio) en modo "forzado" que definan la Configuración de directiva de auditoría avanzada.
2. En la interfaz de la línea de comandos, ejecute el siguiente comando en un controlador de dominio para señalar el GPO ganador:

```
gpresult /scope:computer /h gpo.html
```

3. Modifique la opción correspondiente de Configuración de directiva de auditoría avanzada en el GPO para cumplir con los requisitos mínimos de Tenable Identity Exposure. Por ejemplo:
 - Si Tenable Identity Exposure requiere "Correcto" y el GPO de mayor prioridad define "Error", modifique la opción a "Correcto y error".
 - Si Tenable Identity Exposure requiere "Correcto y error" y el GPO de mayor prioridad define "Correcto", modifique la opción a "Correcto y error".



4. Después de modificar la opción, puede esperar a que se aplique el GPO actualizado o forzarlo con el comando gpupdate.
5. Repita el procedimiento "[Para comprobar la precedencia de los GPO:](#)" para comprobar la nueva política vigente.

Validación del cliente de escucha de registros de eventos

El script de instalación de indicadores de ataque configura un observador de eventos y un productor o consumidor de Instrumental de administración de Windows (WMI) en la memoria de la máquina. WMI es un componente de Windows que le brinda información sobre el estado de los sistemas informáticos locales o remotos.

Para comprobar el registro correcto de WMI:

- Ejecute el siguiente comando en PowerShell:

```
Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter "Filter = '__EventFilter.name='AlsIdForAD-Launcher'"
```

- Si existe al menos un consumidor, obtendrá este tipo de salida:

```
> Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter "Filter = '__EventFilter.name='AlsIdForAD-Launcher'"

__GENUS                : 2
__CLASS                 : __FilterToConsumerBinding
__SUPERCLASS           : __IndicationRelated
__DYNASTY               : __SystemClass
__RELPATH               : 
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name=\"AlsIdForAD-Launcher\",Filter="__EventFilter.Name=\"AlsIdForAD-Launcher"
__PROPERTY_COUNT       : 7
__DERIVATION            : {__IndicationRelated, __SystemClass}
__SERVER               : DC-999
__NAMESPACE            : ROOT\subscription
__PATH                 : \\DC-999\ROOT\subscription:
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name
                          =\"AlsIdForAD-Launcher\",Filter="__EventFilter.Name=\"AlsIdForAD-
Launcher\"
Consumer                : ActiveScriptEventConsumer.Name="AlsIdForAD-Launcher"
CreatorSID              : {1, 1, 0, 0...}
DeliverSynchronously    : False
DeliveryQoS             : 
Filter                  : __EventFilter.Name="AlsIdForAD-Launcher"
MaintainSecurityContext : False
SlowDownProviders       : False
```



```
PSComputerName      : DC-999
```

- Si no hay ningún consumidor de WMI registrado, el comando no devuelve nada.
- Este es un requisito previo para que el proceso se ejecute en el DC para WMI.

Para recuperar el cliente de escucha de registros de eventos (para la versión 3.29 o superior):

- Ejecute el siguiente comando en PowerShell:

```
g cim win32_process | Where-Object { $_.CommandLine -match "Register-TenableADEventsListener.exe" }
```

- Ejemplo de resultado válido:

```
PS C:\IOAInstall> g cim win32_process | Where-Object { $_.CommandLine -match "Register-TenableADEventsListener.exe" }
```

ProcessId	Name	HandleCount	WorkingSetSize	VirtualSize
5748	Register-TenableADEventsListener.exe	152	4096000	4384534528

Para recuperar el proceso de WMI (para la versión 3.19 o superior):

- Ejecute el siguiente comando en PowerShell:

```
g cim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener" }
```

- Ejemplo de resultado válido:

```
> g cim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener" }
```

ProcessId	Name	HandleCount	WorkingSetSize	VirtualSize
952	powershell.exe	502	26513408	2199678185472

Archivos de registros de Tenable Identity Exposure



Si aún no ve alertas de indicadores de ataque después de validar el GPO y el consumidor de WMI, puede revisar los registros internos de Tenable Identity Exposure.

Registro de Ceti

- Busque el siguiente mensaje de error en el registro de CETI:

```
[2022-02-22 22:23:27:570 UTC WARNING] Some domain controllers are not generating IOA events: 'CORP-DC'. {SourceContext="DirectoryEventToCetiAdObjectMessageMapper", DirectoryId=2, Dns="corp.bank.com", Host="10.10.20.10", Source=SYSVOL, Version="3.11.5"}
```

- Si ve este mensaje, verifique que la configuración de GPO y el consumidor de WMI estén en ejecución en el controlador de dominio (DC) que aparece en el mensaje de error anterior.

Opciones de auditoría

- Si ve un error similar al siguiente: “Tenable Identity Exposure requires the Audit Policy...” (Tenable Identity Exposure requiere la política de auditoría...), compruebe los GPO existentes para asegurarse de que no haya definido las políticas de auditoría necesarias en “No Auditing” (Sin auditoría).

```
> 2022-02-10 16:54:21 [2022-02-10 21:54:21:845 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
_ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
|> 2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
|> 2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
|> 2022-02-10 16:54:07 [2022-02-10 21:54:07:849 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
_ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
|> 2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
|> 2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
|> 2022-02-10 16:54:07 [2022-02-10 21:54:07:773 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
_ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
|> 2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
|> 2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
|> 2022-02-10 16:54:07 [2022-02-10 21:54:07:662 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
_ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
```

- Si recibe un error que dice “RSOP...”:



```
[*] RsOP extracted from generated file:
[0cce923c-69ae-11d9-bed3-505054503030] (Audit Directory Service Changes): 3,{0cce921d-69ae-11d9-bed3-505054503030} (Audit File System): 0,{0cce9224-69ae-11d9-bed3-505054503030}
[-] Auditpol output generated at C:\Windows\TEMP\TenableADTask_61fbdaf1f-a644-44a8-873b-6226fac64f15\audit.csv
[-] Auditpol output extracted and converted
[-] No value found in RsOP output for Audit Logoff ({0cce9216-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Sensitive Privilege Use ({0cce9228-69ae-11d9-BED3-505054503030})
[-] No value found in RsOP output for Audit Logon ({0cce9215-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Process Termination ({0cce922c-69ae-11d9-BED3-505054503030})
[-] No value found in RsOP output for Audit Kerberos Service Ticket Operations ({0cce9240-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Kerberos Authentication Service ({0cce9242-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Handle Manipulation ({0cce9223-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit SAM ({0cce9220-69ae-11d9-bed3-505054503030})
[-] Setting value found in auditpol output to Success and Failure for Audit Detailed File Share ({0cce9244-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Process Creation ({0cce922b-69ae-11d9-BED3-505054503030})
[-] No value found in RsOP output for Audit Credential Validation ({0cce923f-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Security Group Management ({0cce9237-69ae-11d9-bed3-505054503030})
[-] No value found in RsOP output for Audit Application Generated ({0cce9222-69ae-11d9-BED3-505054503030})
[-] No value found in RsOP output for Audit Directory Service Access ({0cce923b-69ae-11d9-bed3-505054503030})
[-] Generated audit policies to be deployed: Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion Setting,Setting Value ,System,Audit Logoff,{0c
,System,Audit Credential Validation,{0cce923f-69ae-11d9-bed3-505054503030},Success and Failure,,3 ,System,Audit Security Group Management,{0cce9237-69ae-11d9-bed3-505054503030}
[-] Temporary folder C:\Windows\TEMP\TenableADTask_61fbdaf1f-a644-44a8-873b-6226fac64f15\ cleaned
[-] Running gpupdate /force
[-] Inheritance removed for directory C:\Windows\SYSTEM32\sysvol\alsid.corp\Policies\{765297ad-3ba6-4820-b7f5-ad90dee941e}\Machine\IOA
[-] Authenticated users group removed from IOA folder ACLs
[-] Tenable.ad.service account (S-1-5-21-317789748-3425469236-915459462-2835 : alsid\svc-tenablead) ACL set for IOA folder
[-] Right permissions set to IOA folder
```

- Compruebe las políticas de auditoría y mire el archivo de transcripción en la carpeta SYSVOL para ver si hubo algún problema durante la instalación.

Policy	Setting
Advanced Audit Configuration	
Account Logon	
Audit Credential Validation	Success, Failure
Audit Kerberos Authentication Service	Success, Failure
Audit Kerberos Service Ticket Operations	Success, Failure
DS Access	
Audit Directory Service Access	Success
Logon/Logoff	
Audit Logoff	Success
Audit Logon	Success, Failure

Registro de Cygni

Cygni registra el ataque y enumera el archivo .gz específico al que Tenable Identity Exposure llamó para generar la alerta.

I-DCSync

```
2022-03-15 11:39:31
[2022-03-15 15:39:30:759 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-DCSync' and Event '110052' {SourceContext="AttackEngine", CodeName="I-DCSync", ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-GoldenTicket



```
2022-03-15 11:40:31
[2022-03-15 15:40:31:490 UTC INFORMATION] Anomaly 'Logon' has been raised for Indicator 'I-GoldenTicket' and Event '110061' {SourceContext="AttackEngine", CodeName="I-GoldenTicket", ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ProcessInjectionLsass

```
2022-03-15 12:47:09
[2022-03-15 16:47:09:811 UTC INFORMATION] Anomaly 'ProcessAccess' has been raised for Indicator 'I-ProcessInjectionLsass' and Event '115948' {SourceContext="AttackEngine", CodeName="I-ProcessInjectionLsass", ProfileId=1, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-DCShadow

```
2022-03-15 11:30:30
[2022-03-15 15:30:30:657 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-DCShadow' and Event '109948' {SourceContext="AttackEngine", CodeName="I-DCShadow", ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-BruteForce

```
2022-03-15 08:02:11
[2022-03-15 12:02:11:231 UTC INFORMATION] Anomaly 'An account failed to log on' has been raised for Indicator 'I-BruteForce' and Event '109082' {SourceContext="AttackEngine", CodeName="I-BruteForce", ProfileId=6, AdObjectId="3:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{765297AD-3BAF-4820-B7F5-AD90DEEE941E}\\Machine\\IOA\\dc-vm-10.0.17763-8_.gz", Event.Id=0, Version="3.16.0"}
```

I-PasswordSpraying

```
2022-03-15 12:39:43
[2022-03-15 16:39:43:793 UTC INFORMATION] Anomaly 'An account failed to log on.' has been raised for Indicator 'I-PasswordSpraying' and Event '115067' {SourceContext="AttackEngine", CodeName="I-PasswordSpraying", ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-PetitPotam



```
2022-03-15 12:43:02
[2022-03-15 16:43:02:737 UTC INFORMATION] Anomaly 'PetitPotamEFSError' has been raised for Indicator
'I-PetitPotam' and Event '115844' {SourceContext="AttackEngine", CodeName="I-PetitPotam",
ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ReconAdminsEnum

```
022-03-15 12:55:31
[2022-03-15 16:55:31:638 UTC INFORMATION] Anomaly 'LocalAdmin enumeration (BloodHound/SharpHound).
Version 2016+' has been raised for Indicator 'I-ReconAdminsEnum' and Event '116085'
{SourceContext="AttackEngine", CodeName="I-ReconAdminsEnum", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-Kerberoasting

```
022-03-15 12:51:30
[2022-03-15 16:51:30:236 UTC INFORMATION] Anomaly 'Kerberos TGS requested on honey account' has been
raised for Indicator 'I-Kerberoasting' and Event '116013' {SourceContext="AttackEngine", CodeName="I-
Kerberoasting", ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-
7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-NtdsExtraction

```
2022-03-15 12:03:51
[2022-03-15 16:03:50:949 UTC INFORMATION] Anomaly 'Shadow copy created on 2012 and above' has been
raised for Indicator 'I-NtdsExtraction' and Event '111168' {SourceContext="AttackEngine",
CodeName="I-NtdsExtraction", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

Registro de Cephei

Las siguientes entradas de registro validan que Cephei escriba ataques. El valor de la clave es **attackTypeID**, que especifica el tipo de ataque que puede usar para correlacionar con las entradas de Cygni:

I-DCSync attackTypeID:1

```
2022-03-15 11:39:52
```



```
2022-03-15T15:39:52.037023041Z stdout F [2022-03-15 15:39:52:035 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 32.16 ms : Request Body=
{"timestamp":"1647358722449","directoryId":5,"profileId":4,"attackTypeId":1,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-GoldenTicket attackTypeId:2

```
2022-03-15 11:40:52
2022-03-15T15:40:52.084931986Z stdout F [2022-03-15 15:40:52:084 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.6607 ms : Request Body=
{"timestamp":"1647358773608","directoryId":5,"profileId":4,"attackTypeId":2,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ProcessInjectionLsass attackTypeId:3

```
2022-03-15 12:47:52
2022-03-15T16:47:52.29927328Z stdout F [2022-03-15 16:47:52:298 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 35.7532 ms : Request Body=
{"timestamp":"1647362812784","directoryId":5,"profileId":1,"attackTypeId":3,"count":2}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-DCShadow attackTypeId:4

```
2022-03-15 11:30:52
2022-03-15T15:30:51.949399295Z stdout F [2022-03-15 15:30:51:944 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.2605 ms : Request Body=
{"timestamp":"1647358182800","directoryId":5,"profileId":3,"attackTypeId":4,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-BruteForce attackTypeId:5

```
2022-03-15 08:02:54
2022-03-15T12:02:54.698814039Z stdout F [2022-03-15 12:02:54:698 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 30.7623 ms : Request Body=
{"timestamp":"1647345728023","directoryId":3,"profileId":6,"attackTypeId":5,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PasswordSpraying attackTypeId:6



```
2022-03-15 12:39:52
2022-03-15T16:39:52.187309945Z stdout F [2022-03-15 16:39:52:186 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.9422 ms : Request Body=
{"timestamp":"1647362356837","directoryId":5,"profileId":4,"attackTypeId":6,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PetitPotam attackTypeId:7

```
022-03-15 12:43:52
2022-03-15T16:43:52.226125918Z stdout F [2022-03-15 16:43:52:223 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 15.8402 ms : Request Body=
{"timestamp":"1647362570534","directoryId":5,"profileId":1,"attackTypeId":7,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ReconAdminsEnum attackTypeId:8

```
2022-03-15 12:55:52
2022-03-15T16:55:52.399889635Z stdout F [2022-03-15 16:55:52:399 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 40.6632 ms : Request Body=
{"timestamp":"1647363305295","directoryId":5,"profileId":4,"attackTypeId":8,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-Kerberoasting attackTypeId:10

```
2022-03-15 12:51:52
2022-03-15T16:51:52.352432644Z stdout F [2022-03-15 16:51:52:351 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.0547 ms : Request Body=
{"timestamp":"1647363026345","directoryId":5,"profileId":4,"attackTypeId":10,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-NtdsExtraction attackTypeId:11

```
022-03-15 12:03:52
2022-03-15T16:03:52.137547488Z stdout F [2022-03-15 16:03:52:137 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 13.0304 ms : Request Body=
{"timestamp":"1647360224606","directoryId":5,"profileId":4,"attackTypeId":11,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

Registro de Electra

Debería ver la siguiente entrada:



```
[2022-03-15T14:04:39.151Z] INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-alert (namespace=electra)
```

```
[2022-03-15T14:04:39.151Z] INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-alert (namespace=electra)
[2022-03-15T14:04:39.168Z] INFO: server/4016 on WIN-UQRSCEN0CI3: Sending ws message to listeners. alertIoA (namespace=electra)
```

Registro de Eridanis

Debería ver la siguiente entrada:

```
022-03-15T14:04:39.150Z] INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2010 200 122 - 7ms (namespace=hapi)
[2022-03-15T14:04:39.165Z] INFO: server/4988 on WIN-UQRSCEN0CI3: notifyAttackAndAttackAlertCreation success { attackId: 2011 } (namespace=eridanis)
[2022-03-15T14:04:39.170Z] INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2011 200 122 - 6ms (namespace=hapi)
```

Mitigación de problemas de replicación de DFS

Un parámetro adicional, `-EventLogsFileWriteFrequency X`, en el script de implementación de los indicadores de ataque le permite abordar posibles problemas que pueda experimentar con una replicación lenta o interrumpida del Sistema de archivos distribuido (DFS).

Este parámetro es opcional y Tenable recomienda usarlo solo si tiene problemas de replicación de DFS o los observa desde que implementa el script de IoA. En circunstancias normales, el parámetro permanece en su valor predeterminado y no es necesario incluirlo en la línea de comandos al ejecutar el script.

Cuándo modificar el parámetro

El valor [X] del parámetro `-EventLogsFileWriteFrequency X` es la frecuencia con la que el cliente de escucha de Tenable Identity Exposure genera un archivo de registros de eventos en controladores de dominio (DC) que no son PDCe. El valor predeterminado y recomendado que usa el cliente de escucha de Tenable Identity Exposure es de 15 segundos. Sin embargo, el valor personalizado no se aplica a los controladores de dominio PDCe y permanece en su intervalo predeterminado de 15 segundos para garantizar que las capacidades de detección de ataques estén completamente operativas. Tenable recomienda usar este parámetro y aumentar su valor más allá



de su valor predeterminado de 15 segundos hasta 300 segundos (5 minutos) solo si la infraestructura enfrenta problemas de replicación de DFS o es propensa a ellos.

Recomendaciones

Tenga en cuenta que aumentar la frecuencia de escritura del archivo de registros de eventos hará que el archivo no se genere tan a menudo, lo que aumentará la demora en la detección de ataques (por ejemplo, si el archivo se genera cada 30 segundos en lugar de los 15 segundos predeterminados en los controladores de dominio que no son PDCe). Además, al aumentar el retraso se aumenta el tamaño del archivo de registros de eventos generado dentro de los límites establecidos según lo definido en [Cambios técnicos e impacto potencial](#). Por lo tanto, use este parámetro solo como estrategia de mitigación y no como reemplazo de una investigación adecuada de los problemas de replicación de DFS.

Para aplicar el parámetro:

1. Configure los dominios para los loA como se describe en el procedimiento. Para obtener más información, consulte [Instalar indicadores de ataque](#).



Procedimiento

⚙️ ¿Actualizaciones automáticas en el futuro?

Para evitar tener que reconfigurar manualmente los dominios con cada modificación futura, se recomienda habilitar las actualizaciones automáticas. [Más información](#)



✔️ Tenable.ad aplicará automáticamente los futuros cambios de configuración.
Siga el procedimiento a continuación a fin de configurar los dominios para las actualizaciones automáticas.

1. Descargue el archivo "Register-TenableIOA.ps1".

Descargar

2. Descargue el archivo de configuración de indicadores de ataque para todos los dominios "TadIoaConfig-AllDomains.json".

Descargar

3. Ejecute los siguientes comandos de PowerShell para configurar los dominios:

```
./Register-TenableIOA.ps1 -DomainControllerAddress apjlab-afad-dc-.jp.alsid.corp -TenableServiceAccount svc.alsid@alsid.corp -ConfigurationFileLocation ./TadIoaConfig-AllDomains.json  
./Register-TenableIOA.ps1 -DomainControllerAddress apjlab-dc.alsid.corp -TenableServiceAccount svc.alsid@alsid.corp -ConfigurationFileLocation ./TadIoaConfig-AllDomains.json  
./Register-TenableIOA.ps1 -DomainControllerAddress tk-dcl.tk.jv4u.com -TenableServiceAccount svc.tenablead@tk.jv4u.com -ConfigurationFileLocation ./TadIoaConfig-AllDomains.json  
./Register-TenableIOA.ps1 -DomainControllerAddress dc-vm.tenable.ad -TenableServiceAccount svc.tenablead@tenable.ad -ConfigurationFileLocation ./TadIoaConfig-AllDomains.json  
./Register-TenableIOA.ps1 -DomainControllerAddress dc01.tcorp.local -TenableServiceAccount svc.alsid_priv@tcorp.local -ConfigurationFileLocation ./TadIoaConfig-AllDomains.json
```



2. Abra un terminal de PowerShell con derechos administrativos.
3. Ejecute el script para configurar los controladores de dominio para los loA y agregue el parámetro `-EventLogsFileWriteFrequency X`, donde [X] es la frecuencia que desea establecer para el archivo de registros de eventos.

Retención de registros de eventos de Windows

Si bien Tenable Identity Exposure se esfuerza por procesar tantos registros de eventos de Windows como sea posible para admitir el análisis de seguridad dentro de la funcionalidad de los indicadores de ataque, existen limitaciones técnicas, como la memoria disponible en la máquina que ejecuta los servicios.

El **período de retención global predeterminado** es de 5 minutos. Sin embargo, los registros de eventos específicos de Windows tienen períodos de retención ampliados para mitigar los problemas de correlación que el motor de seguridad podría encontrar:



- SYSMON 5722 y 5723: se retienen durante 6 horas.
- Microsoft-Windows-Security-Auditing/4624: el período de retención de este registro es dinámico, ya que se utiliza ampliamente en indicadores de ataque tanto para la detección como para la correlación. El sistema ajusta la retención en función del uso de la memoria para equilibrar el procesamiento de eventos con los recursos del sistema:
 - **Primera hora:** el servicio de análisis de seguridad aplica el período de retención predeterminado de 5 minutos.
 - **Después de la primera hora,** el sistema evalúa la memoria restante y ajusta la retención de la siguiente manera:
 - Si la memoria disponible es **superior al 50 %:** 1 día.
 - Si la memoria disponible es **del 35 al 50 %:** 6 horas.
 - Si la memoria disponible es **del 20 al 35 %:** 1 hora.
 - Si la memoria disponible es **del 10 al 20 %:** 10 minutos.
 - Si la memoria disponible es **inferior al 10 %:** valor predeterminado de 5 minutos.

Este enfoque dinámico garantiza que el sistema pueda gestionar los eventos entrantes de manera eficiente y, al mismo tiempo, mantenga una memoria adecuada para el análisis de seguridad.

Entradas “desconocidas” en las alertas de indicadores de ataque

En algunos casos, es posible que encuentre entradas “desconocidas” en las alertas de los indicadores de ataque (IoA), como se muestra en la siguiente imagen:

The screenshot displays the Tenable Identity Exposure interface. At the top, it shows the 'Incidentes relacionados con el dominio ALSID' section. A table lists an incident with the following details:

Fecha	Origen	Vector de ataque	Destino	Nombre del ataque	Dominio
2024-03-19 06:03:43	Unknown	La cuenta de ALSID\WSQL_6ec06f289328 se usó para iniciar un ataque DCSync...	dc-vm 10.200.200.4, 10.253.1.3	DCSync	ALSID.CORP Forest (prod)

The incident description includes a YARA rule and a detailed account of the DCSync attack. The MITRE ATT&CK information is as follows:

- Identificador: T1003.006
- Subtécnica de: T1003
- Táctica: TA0006
- Plataforma: Windows
- Permiso necesario: administrador

Estas entradas suelen surgir debido a las siguientes situaciones destacadas:

1. DNS externo fuera de Active Directory (AD)

Si su organización utiliza servidores DNS fuera del dominio de Active Directory (AD), es importante tener en cuenta que el producto no admite entornos DNS que no sean de AD. Es decir, cuando ciertas consultas o solicitudes de DNS se enrutan a través de servidores DNS externos que no forman parte de AD, Tenable Identity Exposure no puede identificarlas, lo que genera entradas “desconocidas” en la lista de alertas de los IoA.

En estos casos, dichos “desconocidos” son esperables y no son indicativos de ningún mal funcionamiento ni error en Tenable Identity Exposure. Esto se debe a la naturaleza de la integración con Active Directory, que exige que los registros de DNS se gestionen en el entorno de AD para lograr una visibilidad y un seguimiento completos.

Solución

- Para minimizar estas entradas “desconocidas”, asegúrese de que la infraestructura de DNS esté completamente integrada en AD para los dominios y recursos que son críticos para la supervisión de la exposición de identidades.
- Si las consultas de DNS deben salir de AD, tenga en cuenta que estos “desconocidos” seguirán apareciendo, ya que Tenable Identity Exposure no puede resolverlos.



2. Permisos insuficientes para la cuenta de Tenable Identity Exposure

Otro motivo para las entradas “desconocidas” en las alertas de los loA podría ser que la cuenta que Tenable Identity Exposure utiliza no tenga permisos suficientes para leer entradas de DNS. El servicio de Tenable Identity Exposure requiere permisos de lectura para acceder a los registros de DNS de Active Directory y analizarlos correctamente.

Soluciones

Para resolver esto, asegúrese de que la cuenta que Tenable Identity Exposure utiliza tenga acceso de lectura a las entradas de DNS necesarias en AD. En concreto, esta cuenta debe tener permiso para consultar los servidores DNS y acceder a los registros necesarios para analizar la exposición de identidades.

Si la cuenta de Tenable Identity Exposure no tiene permisos de lectura adecuados, puede seguir los procedimientos a continuación para otorgarlos.

Consejo: En el script solo es necesario cambiar el nombre de la cuenta que Tenable Identity Exposure utiliza. Los permisos de lectura están incluidos en los siguientes atributos:

- distinguishedName
- dnsRecord (contiene la IP)
- name
- ntSecurityDescriptor
- objectCategory
- objectClass
- objectGUID

Tiene las **dos** opciones siguientes con scripts de PowerShell:

- a. En el administrador de Active Directory, configure el permiso de lectura en el contenedor (dnsZone) y propáguelo a todos los objetos dnsNode secundarios (solución recomendada si corresponde):



```
Import-Module ActiveDirectory

$identity = New-Object System.Security.Principal.NTAccount('EXAMPLE\user2') # Service
account used by TIE for collect/listening
$dnsZonePartition = (Get-ADRootDSE).namingContexts | Where-Object { $_ -match
"DomainDnsZones" }

# dnsRecord attribute GUID
# and Public-Information property set GUID
$guids = @('e0fa1e69-9b45-11d0-afdd-00c04fd930c9', 'e48d0154-bcf8-11d1-8702-
00c04fb96050')

$dnsZones = Get-ADObject -LDAPFilter "(objectClass=dnsZone)" -SearchBase
$dnsZonePartition

ForEach ($dnsZone in $dnsZones) {
    $acl = Get-Acl -Path "AD:\$dnsZone"

    ForEach ($guid in $guids) {
        $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
            $identity,
            [System.DirectoryServices.ActiveDirectoryRights]::ReadProperty,
            [System.Security.AccessControl.AccessControlType]::Allow,
            [guid]$guid,
            [System.DirectoryServices.ActiveDirectorySecurityInheritance]::All,
            [guid]'e0fa1e8c-9b45-11d0-afdd-00c04fd930c9' # dnsZone GUID
        )

        $acl.AddAccessRule($ace)
    }

    # ntSecurityDescriptor
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadControl,
        [System.Security.AccessControl.AccessControlType]::Allow,
        [System.DirectoryServices.ActiveDirectorySecurityInheritance]::All,
        [guid]'e0fa1e8c-9b45-11d0-afdd-00c04fd930c9' # dnsZone GUID
    )

    $acl.AddAccessRule($ace)
    Set-Acl -Path "AD:\$dnsZone" -AclObject $acl
}
}
```

- b. Establezca el permiso de lectura en todos los objetos dnsNode existentes (en el contenedor dnsZone que afecta a todos los objetos dnsNode secundarios):

```
Import-Module ActiveDirectory

$identity = New-Object System.Security.Principal.NTAccount('EXAMPLE\user2') # Service
account used by TIE for collect/listening
$dnsZonePartition = (Get-ADRootDSE).namingContexts | Where-Object { $_ -match
"DomainDnsZones" }
```



```
# dnsRecord attribute GUID
# and Public-Information property set GUID
$guids = @('e0fa1e69-9b45-11d0-afdd-00c04fd930c9', 'e48d0154-bcf8-11d1-8702-00c04fb96050')

$dnsNodes = Get-ADObject -LDAPFilter "(objectClass=dnsNode)" -SearchBase
$dnsZonePartition

ForEach ($dnsNode in $dnsNodes) {
    $acl = Get-Acl -Path "AD:\$dnsNode"

    ForEach ($guid in $guids) {
        $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
            $identity,
            [System.DirectoryServices.ActiveDirectoryRights]::ReadProperty,
            [System.Security.AccessControl.AccessControlType]::Allow,
            [guid]$guid
        )

        $acl.AddAccessRule($ace)
    }

    # ntSecurityDescriptor
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadControl,
        [System.Security.AccessControl.AccessControlType]::Allow
    )

    $acl.AddAccessRule($ace)
    Set-Acl -Path "AD:\$dnsNode" -AclObject $acl
}
}
```

3. Particiones de DNS admitidas

Tenable Identity Exposure no realiza la resolución activa de DNS. En cambio, se basa en entradas de DNS extraídas de las particiones `ForestDnsZones` y `DomainDnsZones`. Si utiliza particiones de DNS personalizadas, Tenable Identity Exposure no las rastrearán ni almacenará sus entradas de DNS.

Indicadores de ataque operativos

Asegurarse de que los procesos de los indicadores de ataque funcionen correctamente es fundamental para que la detección y la respuesta sean precisas. En esta sección se proporcionan instrucciones detalladas para verificar que los componentes de los loA estén operativos y solucionar problemas habituales y con eficacia. Siga los pasos que se indican a continuación para confirmar que todo funcione según lo previsto.



- Asegúrese de que la supervisión de indicadores de ataque (IoA) esté operativa en los controladores de dominio.
 - Verificar la conectividad al dominio: verifique la configuración para asegurarse de que la conectividad al dominio funcione. Para obtener más información, consulte [Dominios](#).
- Verifique la carpeta del GPO de IoA en SYSVOL:
 - Verifique la carpeta del GPO de IoA en el directorio de SYSVOL para confirmar que cada controlador de dominio esté produciendo un archivo `.gz` actualizado.
 - Si algún controlador de dominio no está generando este archivo `.gz`, continúe con los siguientes pasos.
- Confirme que el proceso del cliente de escucha de eventos de IoA se esté ejecutando:
 - Verifique que el proceso `Register-TenableADEventsListener.exe` se esté ejecutando.
 - En las versiones más recientes, este proceso aparece como "Tenable - IOA Events Listener" en el Programador de tareas, además de `Register-TenableADEventsListener.exe`.

Para obtener más información, consulte [Validación del cliente de escucha de registros de eventos](#).
- Si el proceso no se está ejecutando:
 - Asegúrese de que ningún software de EDR o antivirus de los controladores de dominio esté bloqueando el proceso `Register-TenableADEventsListener.exe`.

Para obtener más información, consulte [Detección de antivirus](#).
- Inicie el proceso manualmente:
 - Edite la tarea asociada (`TenableADTask_*`) en el Programador de tareas y haga clic en **Aceptar** para reiniciar el proceso.
- Escale los problemas si persisten: si los pasos anteriores no resuelven el problema, envíe un caso de soporte a Tenable. Es posible que haya un problema subyacente que impida que se ejecute el proceso `Register-TenableADEventsListener.exe`.

Autenticación



Hay varias maneras de autenticar usuarios de Tenable Identity Exposure:

- [Autenticación mediante una cuenta de Tenable Identity Exposure](#)
- [Autenticación mediante LDAP](#)
- [Autenticación mediante SAML](#)

Autenticación mediante Tenable One

Licencia necesaria: Tenable One

Nota: Con una licencia de Tenable One, puede administrar todas las opciones de autenticación de Tenable Vulnerability Management. Para obtener más información, consulte [Access Control \(Control de acceso\) en Tenable Vulnerability Management User Guide](#) (Guía del usuario de Tenable Vulnerability Management).

Para configurar la autenticación mediante Tenable One:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración**.
Aparece el panel "Configuración".
2. En la sección **Autenticación**, haga clic en **Tenable One**.
3. En el cuadro desplegable **Perfil predeterminado**, seleccione el perfil del usuario.
4. En el cuadro **Roles predeterminados**, seleccione los roles del usuario.

Sugerencia: Los usuarios autenticados en Tenable One que no se hayan conectado anteriormente a Tenable Identity Exposure tienen automáticamente una cuenta cuando inician sesión en Tenable Identity Exposure. El perfil y el rol predeterminados se aplican al usuario de manera predeterminada.
Excepción: Los usuarios con el rol "Administrador" en Tenable Vulnerability Management también tienen el rol "Administrador global" en Tenable Identity Exposure.

5. Haga clic en **Guardar**.

Autenticación mediante una cuenta de Tenable Identity Exposure

El método de autenticación más simple es a través de una cuenta de Tenable Identity Exposure que requiere un nombre de usuario y una contraseña.

Este método de autenticación ofrece una política de bloqueo predeterminada, un control de seguridad diseñado para mitigar ataques de fuerza bruta contra los mecanismos de autenticación.



Bloquea las cuentas de usuario después de demasiados intentos fallidos de iniciar sesión. Cuando una cuenta está bloqueada, los usuarios no tienen acceso a las API de Tenable Identity Exposure.

Para configurar la autenticación mediante una cuenta de Tenable Identity Exposure:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración**.
Aparece el panel "Configuración".
2. En la sección **Autenticación**, haga clic en **Tenable Identity Exposure**.
3. En el cuadro desplegable **Perfil predeterminado**, seleccione el perfil del usuario.
4. En el cuadro **Roles predeterminados**, seleccione los roles del usuario.



5. Configure las opciones de la política de bloqueo:

Opción	Descripción	Valor predeterminado
Habilitado	<ul style="list-style-type: none">• Habilitado: Tenable Identity Exposure bloquea la cuenta después de una cantidad determinada de intentos fallidos de iniciar sesión.• Deshabilitado: Tenable Identity Exposure no bloquea la cuenta después de intentos fallidos de iniciar sesión.	Habilitado
Duración del bloqueo	<p>Tiempo durante el cual Tenable Identity Exposure bloquea la cuenta y evita cualquier intento de iniciar sesión. Tenable Identity Exposure desbloquea automáticamente la cuenta una vez transcurrido este tiempo para permitir que el usuario intente iniciar sesión nuevamente.</p> <p>Para configurar la duración del bloqueo:</p> <ol style="list-style-type: none">1. Haga clic en el control deslizante para establecer una duración de bloqueo.2. Seleccione Infinito si no quiere desbloquear la cuenta automáticamente después de un período determinado. <div style="border: 1px solid blue; padding: 5px;"><p>Nota: Si todas las cuentas del grupo "Administrador global" se bloquean, Tenable Identity Exposure desbloquea la cuenta administrativa predeterminada después de 10 segundos.</p></div>	300 segundos
Cantidad de	Cantidad de intentos de inicio de sesión fallidos	3



intentos antes del bloqueo	antes de que Tenable Identity Exposure bloquee la cuenta.	
Período de redención	<p>Intervalo de tiempo durante el cual Tenable Identity Exposure cuenta el número de intentos de inicio de sesión fallidos. Después de una cantidad específica de intentos de inicio de sesión fallidos, Tenable Identity Exposure bloquea la cuenta.</p> <p>Para definir el período de redención:</p> <ol style="list-style-type: none">1. Haga clic en el control deslizante para establecer un intervalo de tiempo.2. Seleccione "Infinito" si no quiere establecer un intervalo de tiempo para contar los intentos de inicio de sesión fallidos antes de que Tenable Identity Exposure bloquee la cuenta.	900 segundos

6. Haga clic en **Guardar**.

Para deshabilitar la política de bloqueo:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración**.

Aparece el panel "Configuración".

2. Haga clic en el conmutador **Habilitado** para desactivar la política de bloqueo.

Nota: Si deshabilita la política de bloqueo, las cuentas de usuario bloqueadas podrán intentar reconectarse.

Para ver la lista de cuentas bloqueadas:



- En Tenable Identity Exposure, vaya a **Cuentas > Gestión de cuentas de usuario**.

En la lista de usuarios, Tenable Identity Exposure muestra las cuentas bloqueadas con un ícono de candado rojo. Tenable Identity Exposure muestra el siguiente mensaje a los usuarios con cuentas bloqueadas: “Su cuenta está bloqueada debido a demasiados intentos de autenticación fallidos. Póngase en contacto con un administrador”.

Para desbloquear una cuenta:

Para poder desbloquear cuentas, tiene que tener permisos para editar usuarios.

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de cuentas de usuario**.

Aparece el panel “Gestión de cuentas de usuario”.

2. En la lista de usuarios, busque la cuenta bloqueada.

3. Haga clic en el ícono del lápiz para editar la cuenta de usuario bloqueada.

Aparece el panel de información del usuario.

4. Haga clic en el botón **Quitar bloqueo**.

Para conceder permisos a los roles de usuario para configurar la política de bloqueo:

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de roles**.

Aparece el panel **Gestión de roles**.

2. Haga clic en el ícono del lápiz junto al nombre de un rol para editarlo.

Aparece el panel **Editar un rol**.

3. Haga clic en la pestaña **Entidades de configuración del sistema**.

4. En la sección **Gestión de permisos**, seleccione la casilla **Política de bloqueo de cuentas**.

5. Haga clic en el conmutador para establecerlo en **Sin autorización** o en **Concedido**.

Un mensaje confirma que Tenable Identity Exposure actualizó los permisos del usuario.

Nota: Tenable Identity Exposure deshabilita la configuración de la política de bloqueo para los usuarios que solo tienen permiso de lectura en este panel.



Autenticación mediante LDAP

Tenable Identity Exposure le permite autenticarse mediante el protocolo ligero de acceso a directorios (LDAP).

Para habilitar la autenticación LDAP, debe tener lo siguiente:

- Una cuenta de servicio preconfigurada con un usuario y una contraseña para acceder a la instancia de Active Directory.
- Un grupo de Active Directory preconfigurado.

Después de configurar la autenticación LDAP, la opción de LDAP aparece en una pestaña en la página de inicio de sesión.

Para configurar la autenticación LDAP:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración**.

Aparece el panel "Configuración".

2. En la sección **Autenticación**, haga clic en **LDAP**.

3. Haga clic en el conmutador **Habilitar autenticación LDAP** para habilitarlo.

Aparece un formulario de información de LDAP.

4. Proporcione la siguiente información:

- En el cuadro **Dirección del servidor LDAP**, escriba la dirección IP del servidor LDAP, comenzando con `ldap://` y terminando con el nombre de dominio y el número de puerto.

Nota: Si usa un servidor LDAPS, escriba la dirección comenzando con `ldaps://` y terminando con el nombre de dominio y el número de puerto. Siga este procedimiento para completar la configuración de LDAPS.

- En el cuadro **Cuenta de servicio utilizada para consultar el servidor LDAP**, escriba el nombre distintivo (DN), SamAccountName o UserPrincipalName que usa para acceder al servidor LDAP.



- En el cuadro **Contraseña de la cuenta de servicio**, escriba la contraseña de esta cuenta de servicio.
- En el cuadro **Base de búsqueda de LDAP**, escriba el directorio de LDAP que Tenable Identity Exposure usa para buscar usuarios que intentan conectarse, comenzando con DC= u OU=. Este puede ser un directorio raíz o una unidad organizativa en particular.
- En el cuadro **Filtro de búsqueda de LDAP**, escriba el atributo que Tenable Identity Exposure usa para filtrar usuarios. Un atributo estándar para la autenticación en Active Directory es sAMAccountname={{nombredeusuario}}. El valor de nombredeusuario es el valor que el usuario proporciona durante la autenticación.

5. Para **Habilitar enlaces SASL**, siga uno de los procedimientos a continuación:

- Si usa SamAccountName para la cuenta de servicio, haga clic en el conmutador **Habilitar enlaces SASL** para **habilitarlo**.
- Si usa el nombre `distintivo` o `UserPrincipalName` para la cuenta de servicio, deje la opción **Habilitar enlaces SASL deshabilitada**.

Consideración importante para Windows Server 2025:

existe una limitación en **Windows Server 2025** donde la configuración de LDAP con enlaces SASL deshabilitados **solo funciona si LDAPS está habilitado**.

Para garantizar una funcionalidad adecuada:

- Si usa **UPN** o **DN** para la cuenta de servicio de Tenable, puede **habilitar los enlaces SASL** en la configuración de LDAP y funcionará correctamente.
- Si prefiere **mantener los enlaces SASL deshabilitados**, debe **habilitar LDAPS** para que LDAP funcione correctamente.

6. En la sección **Perfil y roles predeterminados**, haga clic en **Agregar un grupo de LDAP** para especificar los grupos que pueden autenticarse.

Aparece un formulario de información del grupo de LDAP.

- En el cuadro **Nombre del grupo de LDAP**, escriba el nombre distintivo del grupo (ejemplo: CN=TAD_User,OU=Groups,DC=Tenable,DC=ad).



- En el cuadro desplegable **Perfil predeterminado**, seleccione el perfil del grupo permitido.
- En el cuadro **Roles predeterminados**, seleccione los roles del grupo permitido.

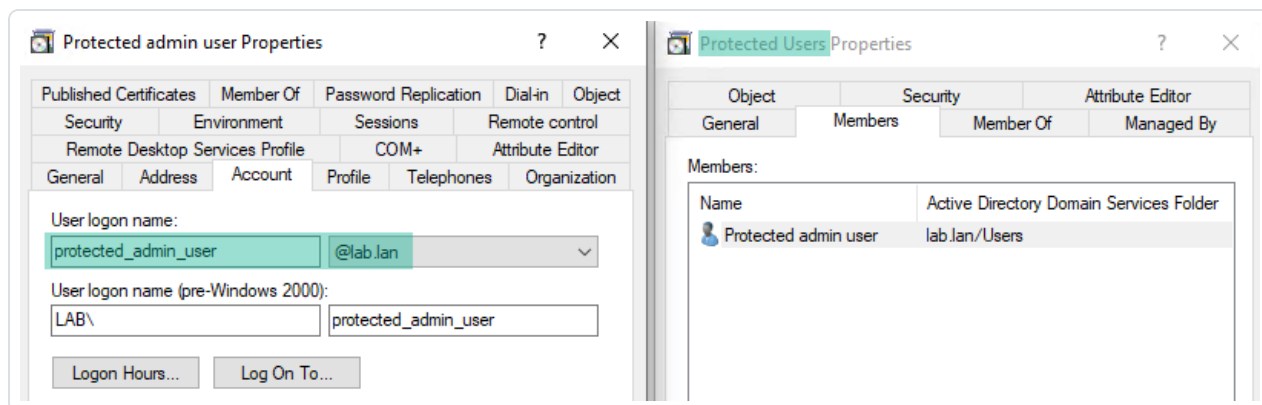
7. Si es necesario, haga clic en **+** para agregar un nuevo grupo permitido.

8. Haga clic en **Guardar**.

Para usar LDAP con miembros del grupo “Usuarios protegidos” en AD:

Dado que los miembros del grupo “Usuarios protegidos” no pueden usar NTLM, tiene que asegurarse de configurar correctamente la autenticación LDAP para utilizar Kerberos en su lugar.

1. **Requisitos previos:** Ya tiene que haber configurado un nombre principal de usuario (UPN) en Microsoft Active Directory. Este es un formato de nombre de usuario similar a una dirección de correo electrónico. Normalmente sigue el formato nombredeusuario@dominio.com, donde “nombredeusuario” es el nombre de la cuenta del usuario y “dominio.com” es el dominio donde se encuentra la cuenta.



2. Inicie sesión en Tenable Identity Exposure con sus credenciales.

3. Configure las siguientes opciones de LDAP:

- Use el FQDN para la dirección del servidor LDAP (asegúrese de que Secure Relay pueda resolverlo).
- Use una cuenta de servicio en formato UPN (por ejemplo, nombredeusuario@dominio.com).



- Establezca el filtro de búsqueda de LDAP en “(userprincipalname={{nombredeusuario}})”.
- Active los enlaces SASL.

LDAP

Habilitar autenticación LDAP



Retransmisión*

Relay



Relay to use to connect to the LDAP server

Dirección del servidor LDAP*

ldap://dc.lab.lan

Cuenta de servicio utilizada para consultar el servidor LDAP*

ldap_svc@lab.lan

Contraseña de la cuenta de servicio*

.....



Base de búsqueda de LDAP*

dc=lab,dc=lan

Filtro de búsqueda de LDAP*

(userprincipalname={{login}})

Habilitar enlaces SASL



PERFIL Y ROLES PREDETERMINADOS

Grupos permitidos

Debe configurar el perfil y los roles predeterminados para cada grupo de LDAP.

#1



Nombre del grupo de LDAP*

CN=ldapusers,CN=Users,DC=lab,DC=lan

Perfil predeterminado*

Tenable



Roles predeterminados*

Usuario ×



4. Inicie sesión en Tenable Identity Exposure usando las credenciales de LDAP como miembro del grupo "Usuarios protegidos" con la sintaxis de nombre principal de usuario.

Tenable Identity Exposure

LDAP SAML

LDAP Account

LDAP Password

Log in

Para agregar un certificado personalizado de una entidad de certificación (CA) de confianza para LDAPS:

1. En Tenable Identity Exposure, haga clic en **Sistema**.
2. Haga clic en la pestaña **Configuración** para mostrar el panel de configuración.
3. En la sección **Servicios de aplicación**, haga clic en **Entidades de certificación de confianza**.
4. En el cuadro **Certificados de CA adicionales**, pegue el certificado de CA de confianza con codificación PEM de su empresa para que Tenable Identity Exposure lo use.



5. Haga clic en **Guardar**.

Problemas de autenticación LDAP

Después de completar y guardar la configuración, la opción de LDAP debería aparecer en la página de inicio de sesión. Para confirmar que la configuración es válida, debe poder iniciar sesión con una cuenta de LDAP.

Mensajes de error

En este punto pueden aparecer dos mensajes de error:

- Hubo un error durante el proceso de autenticación. Vuelva a intentarlo.
 - En este caso, hay un problema con la configuración.
 - Vuelva a comprobar toda la configuración.
 - Compruebe que el servidor donde se hospeda Tenable Identity Exposure pueda acceder al servidor LDAP.
 - Compruebe que la cuenta que se usa para la búsqueda pueda vincularse al servidor LDAP.
 - Para obtener más detalles, consulte los registros de la aplicación.
- El nombre de usuario o la contraseña no son correctos.
 - Verifique que la tecla BLOQ MAYÚS no esté activada y luego vuelva a escribir el nombre de usuario y la contraseña probados.
 - Esto puede deberse a un problema con el filtro de grupo, el filtro de búsqueda o los campos de base de búsqueda.
 - Intente quitar todo filtrado de grupo temporalmente. Para obtener más detalles, consulte los registros de la aplicación.

Para obtener más información sobre los perfiles y roles de seguridad, consulte:

- [Perfiles de seguridad](#)
- [Roles de usuario](#)

Autenticación mediante SAML



Puede configurar la autenticación SAML para que los usuarios de Tenable Identity Exposure puedan usar el inicio de sesión único (SSO) iniciado por el proveedor de identidad al iniciar sesión en Tenable Identity Exposure.

Antes de empezar

- Revise [Tenable SAML Configuration Quick-Reference Guide](#) (Guía de referencia rápida de configuración de SAML de Tenable) para obtener una guía detallada sobre cómo configurar SAML para su uso con Tenable Identity Exposure.
- Compruebe que tiene lo siguiente para el proveedor de identidad (IdP):
 - Solo SAML v2.
 - El cifrado de aserción está habilitado.
 - Grupos de IDP que Tenable Identity Exposure usa para conceder acceso al portal web de Tenable Identity Exposure.
 - URL del servidor SAML.
 - Entidad de certificación (CA) de confianza que firmó el certificado del servidor SAML en formato con codificación PEM, que comienza con -----BEGIN CERTIFICATE ----- y termina con -----END CERTIFICATE -----.

Para configurar la autenticación SAML:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración**.

Aparece el panel "Configuración".

2. En la sección **Autenticación**, haga clic en **Inicio de sesión único SAML**.

3. Haga clic en el conmutador **Habilitar autenticación SAML**.

Aparece un formulario de información de SAML.



Configuración del sistema

Gestión de retransmisiones Gestión de bosques Gestión de dominios Gestión de inquilinos **Configuración** Acerca de Información legal

SERVICIOS DE APLICACIÓN

- > Servidor SMTP
- > Registros de actividad
- > Entidades de certificación de confianza
- > Indicadores de ataque
- > Tenable Cloud
- > Retransmisión
- > Verificación de estado

MOTOR DE ALERTAS

- > SYSLOG
- > Correo electrónico

AUTENTICACIÓN

- > Tenable Identity Exposure
- > LDAP
- > **Inicio de sesión único SAML**

INICIO DE SESIÓN ÚNICO SAML

Habilitar autenticación SAML

Habilite la autenticación SAML para su organización a través de un proveedor de identidades, como Microsoft Entra ID.

URL del servidor SAML*

ENTIDADES DE CERTIFICACIÓN DE CONFIANZA

Copiar y pegar el certificado proporcionado por el servidor SAML

Certificado del servidor SAML*

Certificado de Tenable.ad

Descargar y usar este certificado en el servidor SAML

Activar nueva cuenta de usuario automáticamente

Tras la primera autenticación SAML, active automáticamente la cuenta creada.

PUNTOS DE CONEXIÓN DE TENABLE.AD

URL del proveedor de servicios de Tenable.ad

Punto de conexión de aserción del proveedor de servicios de Tenable.ad

PERFIL Y ROLES PREDETERMINADOS

Grupos permitidos

4. Proporcione la siguiente información:

- En el cuadro **URL del servidor SAML**, escriba la dirección URL completa del servidor SAML del IdP a la que Tenable Identity Exposure debe conectarse.
- En el cuadro **Entidades de certificación de confianza**, pegue la CA que firmó el certificado desde el servidor SAML.



5. En el cuadro **Certificado de Tenable Identity Exposure**, haga clic en **Generar y descargar**. Esto genera un nuevo certificado autofirmado, actualiza la configuración de SAML en la base de datos y devuelve un nuevo certificado para que lo descargue.

Precaución: Cuando hace clic en este botón, la configuración de SAML se ve afectada, ya que Tenable Identity Exposure espera que el IdP se autentique inmediatamente con el certificado generado más recientemente, mientras que el IdP todavía usa un certificado anterior, si existe. Si genera un nuevo certificado de Tenable Identity Exposure, tiene que reconfigurar el IdP para que use el nuevo certificado.

6. Haga clic en el conmutador **Activar nueva cuenta de usuario automáticamente** para activar las nuevas cuentas de usuario después del primer inicio de sesión con SAML.
7. En **Puntos de conexión de Tenable Identity Exposure**, proporcione la siguiente información:
 - URL del proveedor de servicios de Tenable Identity Exposure
 - Punto de conexión de aserción del proveedor de servicios de Tenable Identity Exposure
8. En la sección **Perfil y roles predeterminados**, haga clic en **Agregar un grupo de SAML** para especificar los grupos que pueden autenticarse.

Aparece un formulario de información del grupo de SAML.

9. Proporcione la siguiente información:
 - En el cuadro **Nombre del grupo de SAML**, escriba el nombre del grupo permitido tal como aparece en el servidor SAML.
 - En el cuadro desplegable **Perfil predeterminado**, seleccione el perfil del grupo permitido.
 - En el cuadro **Roles predeterminados**, seleccione los roles del grupo permitido.
10. Si es necesario, haga clic en **+** para agregar un nuevo grupo permitido.

11. Haga clic en **Guardar**.

Después de configurar la autenticación SAML, la opción de SAML aparece en una pestaña en la página de inicio de sesión.

Para obtener más información sobre los perfiles y roles de seguridad, consulte:



- [Perfiles de seguridad](#)
- [Roles de usuario](#)

Cuentas de usuario

La página **Gestión de cuentas de usuario** da la posibilidad de agregar, editar, eliminar o ver los detalles de las cuentas de usuario de Tenable Identity Exposure.

Los usuarios pertenecen a dos categorías:

- Administrador global: rol de administrador que incluye todos los permisos.
- Usuario: rol de usuario simple únicamente con permisos de solo lectura de los datos empresariales.

Precaución

Si tiene una **licencia de Tenable Identity Exposure independiente**, puede elegir enviar datos a la plataforma Tenable por medio de las opciones. Al hacer esto, activa las funcionalidades Identidad 360 y Motor de seguridad de Tenable Identity Exposure.

Para facilitar la comunicación con la plataforma Tenable y rastrear las acciones de los usuarios, Tenable Identity Exposure crea automáticamente los siguientes objetos en la plataforma Tenable, visibles en las opciones del contenedor de Tenable Vulnerability Management :

- Un grupo denominado con el patrón TIE - Autogenerated users - {cadena_aleatoria}.
- Un permiso denominado TIE - Autogenerated - Can view all assets - {cadena_aleatoria} aplicado al grupo TIE - Autogenerated users - {cadena_aleatoria}. Permite a los usuarios ver los activos que Tenable Identity Exposure exportó a la plataforma Tenable.
- Para cada usuario de Tenable Identity Exposure, un usuario denominado según el patrón tie-{nombre_de_usuario}-{cadena_aleatoria} que es miembro del grupo TIE - Autogenerated users - {cadena_aleatoria}. Este usuario tiene una contraseña aleatoria segura y **no** debe usarla para autenticarse en el contenedor de Tenable Vulnerability Management. Tiene derechos básicos de solo lectura en el contenedor de Tenable Vulnerability Management.

Un administrador puede ver estos objetos, pero **no debe modificarlos**, ya que los cambios podrían interrumpir las funcionalidades Identidad 360 y Motor de seguridad.



Para crear un usuario:

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de cuentas de usuario**.

Aparece el panel **Gestión de cuentas de usuario**.

2. Haga clic en el botón **Crear un usuario** a la derecha.

Aparece el panel **Crear un usuario**.

3. En la sección **Información principal**, escriba la siguiente información sobre el usuario:

- Nombre
- Apellido(s)
- Correo electrónico
- Contraseña: requiere un mínimo de 12 caracteres con al menos 1 minúscula, 1 mayúscula, 1 número y 1 carácter especial
- Confirmación de contraseña
- Departamento
- Biografía

4. Haga clic en el conmutador **Permitir autenticación** para activar el usuario.

5. En la sección **Gestión de roles**, seleccione un rol para aplicárselo al usuario.


6. Haga clic en **Crear**.

Un mensaje confirma que Tenable Identity Exposure creó el usuario con el rol seleccionado.

Para editar un usuario:

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de cuentas de usuario**.

Aparece el panel **Gestión de cuentas de usuario**.

2. En la lista de usuarios, pase el cursor por la línea donde aparece el nombre del usuario y haga clic en el ícono  al final de la línea.

Aparece el panel **Editar un usuario**.



3. En la sección **Información principal**, modifique la siguiente información sobre el usuario según sea necesario:

- Nombre
- Apellido(s)
- Correo electrónico
- Contraseña: requiere al menos 8 caracteres
- Confirmación de contraseña
- Departamento
- Biografía

4. En la sección **Gestión de roles**, modifique el rol del usuario según sea necesario.


5. Haga clic en **Editar**.

Un mensaje confirma que Tenable Identity Exposure actualizó el usuario con el rol seleccionado.

Para desactivar un usuario:

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de cuentas de usuario**.

Aparece el panel **Gestión de cuentas de usuario**.

2. En la lista de usuarios, pase el cursor por la línea donde aparece el nombre del usuario y haga clic en el ícono  al final de la línea.

Aparece el panel **Editar un usuario**.

3. Haga clic en el conmutador **Permitir autenticación** para desactivar el usuario.

4. Haga clic en **Editar**.


Un mensaje confirma que Tenable Identity Exposure actualizó el usuario.

Para eliminar un usuario:



1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de cuentas de usuario**.

Aparece el panel **Gestión de cuentas de usuario**.

2. En la lista de usuarios, pase el cursor por la línea donde aparece el nombre del usuario que quiere eliminar y haga clic en el ícono  al final de la línea.

Aparece un mensaje para pedirle que confirme la eliminación.

3. Haga clic en **Eliminar**.

Un mensaje confirma que Tenable Identity Exposure eliminó el usuario.

Perfiles de seguridad

Rol de usuario obligatorio: administrador o usuario de la organización con permisos apropiados.

Los perfiles le permiten crear y personalizar su propia vista de los riesgos que afectan a su instancia de Active Directory.

Cada perfil muestra los escenarios de exposición y ataque configurados para los usuarios que tienen ese perfil. Por ejemplo, la vista general del análisis de datos de un administrador de TI puede ser diferente de la del equipo de seguridad, que muestra una vista integral de todos los riesgos que enfrentan las infraestructuras de AD.

La aplicación de un perfil de seguridad permite que distintos tipos de usuarios revisen el análisis de datos desde diferentes ángulos, según lo que definan los indicadores de ese perfil de seguridad.

El panel "Gestión de perfiles de seguridad" le permite mantener distintos tipos de usuarios que pueden revisar el análisis de seguridad desde diferentes ángulos. Además, los perfiles de seguridad le permiten personalizar el comportamiento de los indicadores de exposición y los indicadores de ataque.

Nota: Tenable Identity Exposure brinda un perfil de seguridad predeterminado llamado "Tenable". **No es posible modificar ni eliminar el perfil Tenable**, pero se puede usar como plantilla para crear otros perfiles de seguridad con opciones ajustadas según sus necesidades.

Para crear un nuevo perfil de seguridad:



1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de perfiles de seguridad**.

Aparece el panel **Gestión de perfiles de seguridad**.

2. Haga clic en el botón **Crear un perfil** a la derecha.

Aparece el panel **Crear un perfil**.

3. Desde el cuadro desplegable "Acción", puede:

- **Crear un perfil nuevo**.
- **Copiar** un perfil de seguridad existente (por ejemplo, el perfil "Tenable") desde el cual puede crear un nuevo perfil.

4. En el cuadro **Nombre del nuevo perfil**, escriba un nombre para el nuevo perfil.

Nota: Tenable Identity Exposure solo acepta caracteres alfanuméricos y guiones bajos.


5. Haga clic en el botón **Crear** en la esquina inferior derecha.

Un mensaje indica que Tenable Identity Exposure creó el perfil. Aparece el panel **Configuración del perfil**.

Para eliminar un perfil de seguridad:

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de perfiles de seguridad**.

Aparece el panel **Gestión de perfiles de seguridad**.

2. En la lista de perfiles de seguridad, pase el cursor por el perfil de seguridad que quiere eliminar y haga clic en el ícono  al final de la línea.

Aparece un mensaje para pedirle que confirme la eliminación.

3. Haga clic en **Eliminar**.

Un mensaje confirma que Tenable Identity Exposure eliminó el perfil.

Qué hacer a continuación

Para completar la creación del perfil, consulte [Personalizar un indicador](#) para obtener más información.

Para obtener más información, consulte:



- [Personalizar un indicador](#)
- [Ajustar la personalización de un indicador](#)


Personalizar un indicador

Rol de usuario obligatorio: administrador o usuario de la organización con permisos apropiados.


Puede personalizar los indicadores de exposición y los indicadores de ataque para un perfil de seguridad.

Cada perfil de seguridad funciona de forma independiente para garantizar que un perfil no afecte a los resultados de otro. Debe usar el perfil "Tenable" únicamente como referencia, ya que no puede personalizarlo ni usarlo para permitir anomalías. Tiene que crear sus propios perfiles personalizados para cumplir con requisitos específicos.

El término "Personalización global" en el panel de personalización del indicador **hace referencia a todos los dominios** y no a todos los perfiles. En consecuencia, cualquier opción que aplique a la "Personalización global" para un perfil de seguridad no influirá en el perfil "Tenable" ni en otro perfil.

Sugerencia: Para ver las opciones del perfil de seguridad "Tenable", haga clic en el ícono  al final de la línea.

Para personalizar un indicador:

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de perfiles de seguridad**.
Aparece el panel **Gestión de perfiles de seguridad**.
2. En la lista de perfiles de seguridad, pase el cursor por el perfil de seguridad que contiene el indicador que quiere personalizar. Haga clic en el ícono  al final de la línea donde aparece el nombre del archivo del perfil de seguridad.
Aparece el panel **Configuración del perfil**.
3. Seleccione la pestaña **Indicadores de exposición** o **Indicadores de ataque**.
4. (Opcional) En el cuadro **Buscar un indicador**, escriba el nombre de un indicador.
5. Haga clic en el nombre de un indicador para personalizarlo.



Aparece el panel **Personalización del indicador**.

6. Seleccione las opciones de la tabla "Opciones".

Sugerencia: Para habilitar el **modo agresivo** para los indicadores de ataque, haga clic en el botón de alternancia y establezca la opción "Modo agresivo" en "Sí".

Sugerencia: Algunas opciones del indicador requieren el uso de expresiones regulares (regex). Las regex son una coincidencia de tipo "contiene" en lugar de una coincidencia de tipo "es igual".

- Para obtener una coincidencia exacta, debe usar la sintaxis de caracteres especiales de regex ("^...\$").

- Además, al usar regex, debe escapar los caracteres especiales con una barra invertida. Ejemplo: Para declarar "domain\user" y "CN=Vincent C (Test),DC=tenable,DC=corp", escriba "domain\user" y "CN=Vincent C. \ (Test\),DC=tenable,DC=corp".

7. Haga clic en **Guardar como borrador**.

Un mensaje confirma que Tenable Identity Exposure guardó las opciones de personalización.

Para aplicar la personalización:

1. Puede seguir uno de estos procedimientos:

- En el panel **Configuración del perfil**, haga clic en **Aplicar personalización pendiente** en la esquina inferior derecha.
- En el panel **Gestión de perfiles de seguridad**, haga clic en el ícono ✓ al final de la línea donde aparece el nombre del perfil de seguridad.


Aparece un mensaje para advertirle que, al aplicar la personalización, se borran todos sus datos y se requiere un análisis completo de la instancia de Active Directory supervisada, lo que puede llevar algún tiempo.

2. Haga clic en **Aceptar**.

Un mensaje confirma que Tenable Identity Exposure aplicó las opciones de personalización. En la columna *Análisis de seguridad* de la tabla **Gestión de perfiles de seguridad**, **En espera** indica que el análisis según su perfil de seguridad está a la espera de ejecutarse.

Para descartar la personalización:



- Puede seguir uno de estos procedimientos:
 - En el panel **Configuración del perfil**, haga clic en **Revertir personalización pendiente** en la esquina inferior derecha.
 - En el panel **Gestión de perfiles de seguridad**, haga clic en el ícono  al final de la línea donde aparece el nombre del perfil de seguridad.

Un mensaje confirma que Tenable Identity Exposure canceló las opciones de personalización.

Consulte también


- [Ajustar la personalización de un indicador](#)

Ajustar la personalización de un indicador

Rol de usuario obligatorio: administrador o usuario de la organización con permisos apropiados.

La personalización adicional de un indicador para un perfil de seguridad le permite seleccionar opciones de indicador para dominios específicos. De manera predeterminada, la personalización global se aplica a todos los dominios.

Para ajustar la personalización de un indicador:

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de perfiles de seguridad**.
Aparece el panel **Gestión de perfiles de seguridad**.
2. En la lista de perfiles de seguridad, pase el cursor por el perfil de seguridad que contiene el indicador que quiere personalizar. Haga clic en el ícono  al final de la línea donde aparece el nombre del archivo del perfil de seguridad.
Aparece el panel **Configuración del perfil**.
3. Seleccione la pestaña **Indicadores de exposición** o **Indicadores de ataque**.
4. (Opcional) En el cuadro **Buscar un indicador**, escriba el nombre de un indicador.
5. Haga clic en el nombre de un indicador para personalizarlo.
Aparece el panel **Personalización del indicador**.



6. Junto a la pestaña **Personalización global**, haga clic en el ícono **+**.
Aparece una pestaña **Personalización n.º 1**.
7. Haga clic en el cuadro **Aplicar en**.
Aparece el panel **Bosques y dominios**.
8. (Opcional) En el cuadro de búsqueda, escriba el nombre de un bosque o dominio.
9. Seleccione el dominio.
10. Haga clic en **Filtrar selección**.
11. Siga personalizando el indicador para el dominio seleccionado según sea necesario.
12. Haga clic en **Guardar como borrador**.

Para descartar la personalización ajustada:

1. Haga clic en la pestaña de la personalización.
2. Haga clic en **Quitar esta configuración** al final del panel.

Consulte también

- [Personalizar un indicador](#)

Roles de usuario

Tenable Identity Exposure usa el control de acceso basado en roles (RBAC) para proteger el acceso a los datos y las funciones dentro de su organización. Los roles determinan el tipo de información a la que un usuario puede acceder desde su cuenta en función de su rol.

Los usuarios con los permisos adecuados pueden asignar permisos a otros usuarios según su rol para realizar las siguientes acciones:

- Leer contenido y menús, y configuraciones del sistema y de indicadores de exposición.
- Editar contenido y menús, y configuraciones del sistema y de indicadores de ataque.
- Crear cuentas, perfiles de seguridad y roles.



Consulte también


- [Gestionar roles](#)
- [Establecer permisos para un rol](#)
- [Establecer permisos en entidades de la interfaz de usuario \(ejemplo\)](#)

Gestionar roles


Para crear un nuevo rol:

1. En Tenable Identity Exposure, vaya a **Cuentas > Gestión de roles**.
2. Haga clic en el botón **Crear un rol** en la esquina superior derecha.
Aparece el panel **Crear un rol**.
3. En el cuadro "Nombre", escriba el nombre para el rol.
4. En el cuadro "Descripción", escriba información sobre el rol.
5. Haga clic en **Agregar** en la esquina inferior derecha.

Aparece un mensaje para confirmar que Tenable Identity Exposure creó el rol. Aparece el panel **Editar un rol** para que establezca los permisos para el rol.

Nota: No se puede modificar el rol de administrador de Tenable Identity Exposure (llamado "Administrador global"). Haga clic en el ícono  para mostrar las opciones del rol de Tenable Identity Exposure.

Para eliminar un rol:

1. En Tenable Identity Exposure, vaya a **Cuentas > Gestión de roles**.
2. En la lista de roles, pase el cursor por el rol que quiere eliminar y haga clic en el ícono  a la derecha.
Aparece un mensaje para pedirle que confirme la eliminación.
3. Haga clic en "Eliminar".
Aparece un mensaje para confirmar la eliminación del rol.

Consulte también




- [Establecer permisos para un rol](#)

Establecer permisos para un rol

Rol de usuario obligatorio: administrador o usuario de la organización con permisos apropiados.

Tenable Identity Exposure usa el control de acceso basado en roles (RBAC) para proteger el acceso a los datos. Un rol determina a qué tipo de información pueden acceder los usuarios según sus roles funcionales dentro de la organización. Cuando crea un nuevo usuario en Tenable Identity Exposure, le asigna a ese usuario un rol específico con sus permisos asociados.

Para establecer permisos para un rol:

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de roles**.
2. Pase el cursor por el rol para el cual quiere establecer permisos y haga clic en el ícono  a la derecha.


Aparece el panel **Editar un rol**.

3. En **Gestión de permisos**, seleccione un tipo de entidad:
 - [Entidades de datos](#)
 - [Entidades de usuario](#)
 - [Entidades de configuración del sistema](#)
 - [Entidades de interfaz](#)
4. En la lista de nombres de entidades, seleccione la entidad en la que va a establecer los permisos.
5. En las columnas **Leer**, **Editar** o **Crear**, haga clic en el conmutador correspondiente para establecerlo en "Concedido" o "Sin autorización".
6. Puede seguir uno de estos procedimientos:
 - Hacer clic en "Aplicar" para aplicar el permiso y mantener abierto el panel **Editar un rol** para realizar más modificaciones.
 - Hacer clic en "Aplicar y cerrar" para aplicar el permiso y cerrar el panel **Editar un rol**.

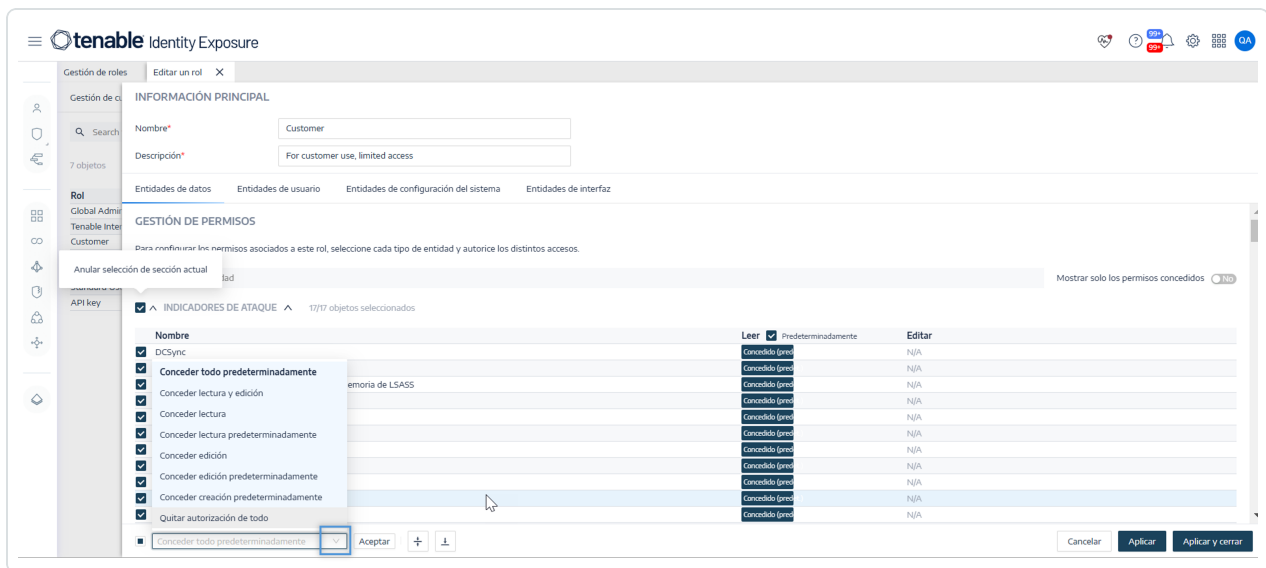
Un mensaje confirma que Tenable Identity Exposure actualizó el rol.



Para establecer permisos en masa para un rol:

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de roles**.
2. Pase el cursor por el rol para el cual quiere establecer permisos y haga clic en el ícono  a la derecha.
Aparece el panel **Editar un rol**.
3. En **Gestión de permisos**, seleccione un tipo de entidad.
4. Seleccione las entidades o secciones de entidades (por ejemplo, indicadores de exposición) para establecer permisos.
5. Al final de la página, haga clic en la flecha del cuadro desplegable para mostrar una lista de permisos.
6. Seleccione los permisos para el rol.
7. Haga clic en **Aceptar**.

Un mensaje confirma que Tenable Identity Exposure estableció los permisos en las entidades.



Tipos de permisos

Permiso	Descripción
Leer	Permiso para ver un objeto o una configuración.



Editar	Permiso para modificar un objeto o una configuración. Requiere el permiso Leer para aplicar modificaciones.
Crear	Permiso para crear un objeto o una configuración. El permiso Crear requiere los permisos Leer y Editar para realizar acciones permitidas en los recursos permitidos.

Tipos de entidades

Hay cuatro tipos de entidades en Tenable Identity Exposure que requieren permisos de acceso que puede adaptar para cada rol de usuario en su organización:

Tipo de entidad	Contiene	Permisos
Entidades de datos		
Esta entidad controla los permisos para configurar la instancia de Active Directory supervisada y configurar el análisis de datos en Tenable Identity Exposure.	<ul style="list-style-type: none">• Indicadores de ataque• Indicadores de exposición• Bosques• Dominios• Perfiles• Usuarios• Alertas por correo electrónico• Alertas por SYSLOG• Roles• Entidad Relay• Informes	Leer, Editar, Crear
Entidades de usuario		
Esta entidad controla la capacidad de	<ul style="list-style-type: none">• Preferencias	Editar, Crear



<p>un usuario de configurar la información que Tenable Identity Exposure muestra para el análisis de datos y de modificar la información y las preferencias personales.</p>	<ul style="list-style-type: none">• Tableros de control• Widgets• Clave de API• Información personal	
Entidades de configuración del sistema		
<p>Esta entidad controla el acceso a la plataforma y a los servicios de Tenable Identity Exposure.</p>	<ul style="list-style-type: none">• Servicios de aplicación (SMTP, registros, autenticación en Tenable Identity Exposure, indicadores de ataque, entidades de certificación de confianza)• Puntuaciones a través de API pública• Licencias• Autenticación LDAP• Autenticación SAML <div data-bbox="800 1234 1203 1514" style="border: 1px solid blue; padding: 5px;"><p>Nota: Los permisos para la autenticación LDAP y SAML no están disponibles si tiene una licencia de Tenable Vulnerability Management.</p></div> <ul style="list-style-type: none">• Topología• Política de bloqueo de cuentas• Volver a rastrear dominios• Registros de actividad	<p>Leer, Editar</p>



	<ul style="list-style-type: none">• Servicio de Tenable Cloud (Recopilación de datos de Tenable Cloud)• Compatibilidad con Microsoft Entra ID• Verificaciones de estado• Mostrar solo los rastros del usuario	
Entidades de interfaz		
Esta entidad define los permisos para acceder a partes específicas de la interfaz de usuario y las funcionalidades de Tenable Identity Exposure.	Rutas de acceso a funcionalidades específicas de Tenable Identity Exposure. Para obtener más información, consulte Establecer permisos en entidades de la interfaz de usuario (ejemplo) .	Concedido, Sin autorización

Consulte también

- [Cuentas de usuario](#)
- [Roles de usuario](#)

Establecer permisos en entidades de la interfaz de usuario (ejemplo)


Tenable Identity Exposure aplica permisos para la ruta usada para acceder a una determinada funcionalidad de la interfaz de usuario. En el siguiente ejemplo se muestra cómo establecer permisos para permitir la configuración de SYSLOG.

Para acceder a los parámetros de SYSLOG, los usuarios necesitan permisos para la ruta **Sistema > Configuración > SYSLOG** en Tenable Identity Exposure:

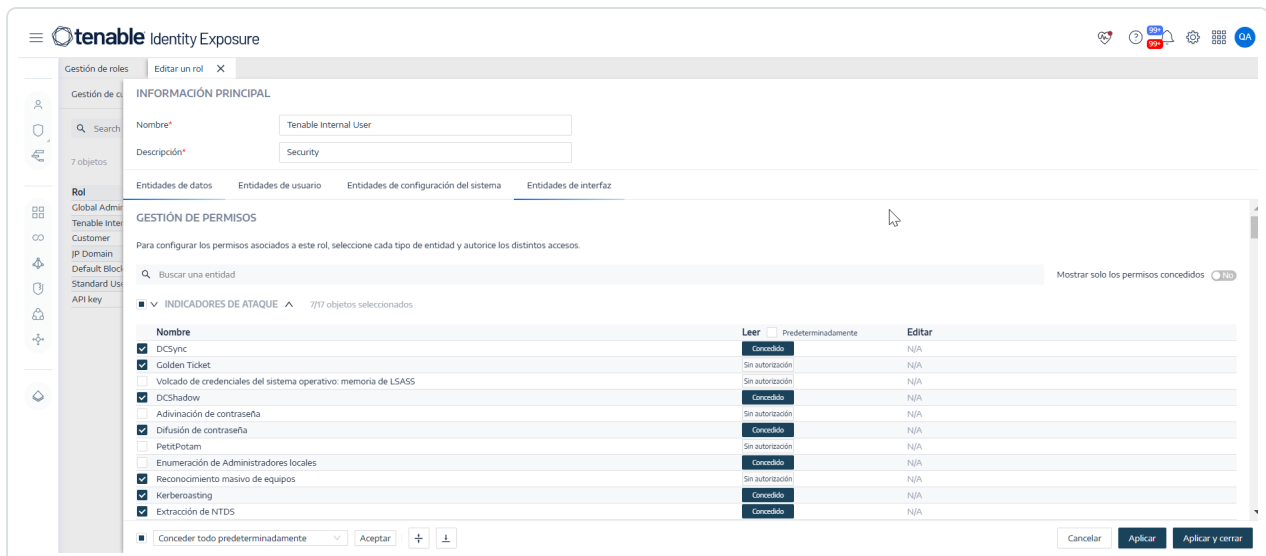
- Configuración del sistema: **Gestión > Sistema**
- Parámetros de configuración: **Gestión > Sistema > Configuración**
- Alertas de SYSLOG: **Gestión > Sistema > Configuración > Motor de alertas > SYSLOG**



Para establecer permisos para la configuración de SYSLOG:

1. En Tenable Identity Exposure, haga clic en **Cuentas > Gestión de roles**.
2. Pase el cursor por el rol para el cual quiere establecer permisos y haga clic en el ícono  a la derecha.
Aparece el panel **Editar un rol**.
3. En **Gestión de permisos**, seleccione **Entidades de interfaz**.
4. En la lista de entidades, haga lo siguiente:
 - Seleccione **Gestión > Sistema** y haga clic en el conmutador "Acceso" para establecerlo en **Concedido**.
 - Seleccione **Gestión > Sistema > Configuración** y haga clic en el conmutador "Acceso" para establecerlo en **Concedido**.
 - Seleccione **Gestión > Sistema > Configuración > Motor de alertas > SYSLOG** y haga clic en el conmutador "Acceso" para establecerlo en **Concedido**.
5. Haga clic en **Aplicar**.

Un mensaje confirma que Tenable Identity Exposure actualizó los permisos en las entidades.



6. En **Gestión de permisos**, seleccione **Entidades de datos**.
7. En la lista de secciones de entidades, seleccione **Alertas por SYSLOG**.

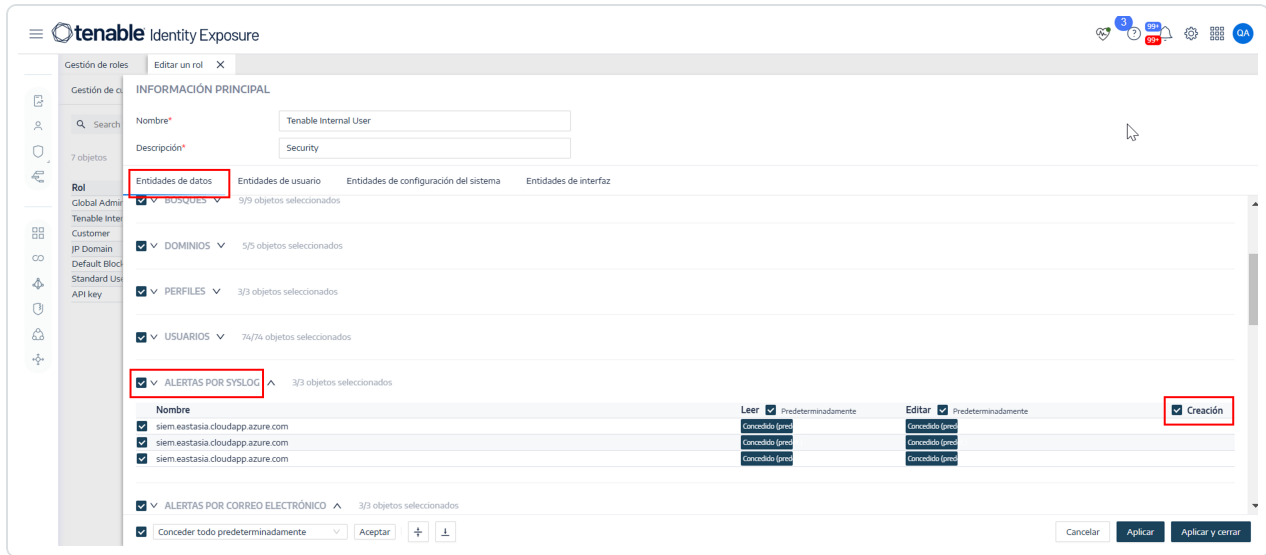


8. Seleccione el permiso **Creación**.

Tenable Identity Exposure concede implícitamente los permisos de lectura y edición.

9. Haga clic en **Aplicar y cerrar**.

Un mensaje confirma que Tenable Identity Exposure actualizó los permisos en las entidades.



Bosques

Un bosque de Active Directory (AD) es una colección de dominios que comparten un esquema, una configuración y relaciones de confianza en común. Proporciona una estructura jerárquica para gestionar y organizar recursos, lo que permite la administración centralizada y la autenticación segura en varios dominios dentro de una organización.

Gestionar los bosques

Para agregar un bosque:

1. En Tenable Identity Exposure, haga clic en **Sistema > Gestión de bosques**.
2. Haga clic en **Agregar un bosque** a la derecha.
Aparece el panel "Agregar un bosque".
3. En el cuadro **Nombre**, escriba el nombre del bosque.



4. En la sección **Cuenta**, indique lo siguiente para la cuenta de servicio que Tenable Identity Exposure usa:


- **Nombre de usuario:** escriba el nombre de la cuenta de servicio.
Formato: nombre principal de usuario, como "tenablead@dominio.ejemplo.com" (se recomienda para la compatibilidad con [Autenticación de Kerberos](#)); o NetBIOS, como "NombreDominioNetBIOS\NombreCuentaSam".
- **Contraseña:** escriba la contraseña de la cuenta de servicio.

Nota: Si tiene que definir la cuenta de servicio de AD de Tenable Identity Exposure como miembro del grupo "Usuarios protegidos", asegúrese de que la configuración de Tenable Identity Exposure admita [Autenticación de Kerberos](#), ya que "Usuarios protegidos" no puede usar la autenticación de NTLM.

5. Haga clic en **Agregar**.

Un mensaje confirma la adición de un nuevo bosque.

Para editar un bosque:

1. En Tenable Identity Exposure, haga clic en **Sistema > Gestión de bosques**.
2. En la lista de bosques, pase el cursor por el bosque que quiere modificar y haga clic en el ícono  a la derecha.

Aparece el panel **Editar un bosque**.

3. Haga las modificaciones que considere necesarias.
4. Haga clic en **Editar**.

Un mensaje confirma que Tenable Identity Exposure actualizó el bosque.

Proteger cuentas de servicio

Para proteger las cuentas de servicio con el fin de mantener la seguridad, Tenable recomienda configurar correctamente los atributos de Control de cuentas de usuario (UAC) para evitar la delegación, exigir la autenticación previa, usar un cifrado más seguro, aplicar requisitos y vencimiento de contraseñas y permitir cambios de contraseñas autorizados. Estas medidas mitigan



el riesgo de acceso no autorizado y posibles vulneraciones de seguridad, lo que garantiza la integridad de los sistemas y los datos de una organización.

Para modificar las opciones mediante un editor de políticas de Windows:

Puede modificar las opciones de control de cuentas de usuario mediante el Editor de directivas de seguridad local o el Editor de directivas de grupo local de Windows con los privilegios administrativos adecuados.

- En el editor, vaya a **Directivas locales** -> **Opciones de seguridad** para buscar y configurar las siguientes opciones (pueden variar según la versión de Windows):
 - *“Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de red”*: establezca esta opción en **Habilitado**.
 - *“Cuentas: No requerir la preautenticación de Kerberos”*: establezca esta opción en **Deshabilitado**.
 - *“Seguridad de red: Configurar los tipos de cifrado permitidos para Kerberos”*: asegúrese de que la opción *“Usar tipos de cifrado DES de Kerberos para esta cuenta”* **no** esté seleccionada.
 - *“Cuentas: Vigencia máxima de la contraseña”*: establezca el período de vencimiento de la contraseña (por ejemplo, 30, 60 o 90 días para que `PasswordNeverExpires = FALSE`).
 - *“Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola”*: establezca esta opción en **Deshabilitado**.
 - *“Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché (si un controlador de dominio no está disponible)”*: establezca el valor deseado, como “10”, para permitir que los usuarios cambien las contraseñas.

Para modificar la configuración mediante PowerShell:

- En una máquina que hospeda AD, abra PowerShell con los privilegios administrativos adecuados y ejecute el siguiente comando:

```
Set-ADAccountControl -Identity <AD_ACCOUNT> -AccountNotDelegated $true -UseDESKeyOnly $false -DoesNotRequirePreAuth $false -PasswordNeverExpires $false -PasswordNotRequired $false -CannotChangePassword $false
```



Donde <AD_ACCOUNT> es el nombre de la cuenta de Active Directory que quiere modificar.

Dominios

Tenable Identity Exposure supervisa dominios que agrupan objetos que comparten configuraciones comunes de manera lógica para una gestión centralizada.

Para agregar un dominio:

1. En Tenable Identity Exposure, haga clic en **Sistema**.
2. Haga clic en la pestaña **Gestión de dominios**.
Aparece el panel **Gestión de dominios**.
3. Haga clic en **Agregar un dominio** en la esquina superior derecha.
Aparece el panel **Agregar un dominio**.

tenable Identity Exposure

Gestión de dominios | Agregar un dominio X

Gestión de re

Buscar

5 objetos

Nombre

ALSID

Japan Domai

KHLAB

TCORP Dom

TKLab

INFORMACIÓN PRINCIPAL

Nombre*
Nombre del dominio

FQDN del dominio*
Ejemplo: dominio.local

Bosque*
Bosque al que pertenece este dominio

Retransmisión*
Retransmisión a la que pertenece este dominio

Análisis con privilegios
Al activar esta característica, indica que la cuenta `svc.alsid@alsid.corp` establecida en este bosque puede recopilar datos con privilegios de este dominio, como hashes de contraseñas. Estos datos se usarán para realizar análisis de seguridad adicionales. Esto es opcional ⓘ

Transferencia de análisis con privilegios
Elegió transferir los datos con privilegios al servicio de Tenable Cloud. Puede cambiar esta opción para todos los dominios en [Configuración de Tenable Cloud](#).

CONTROLADOR DE DOMINIO PRINCIPAL

Dirección IP o FQDN*
Dirección IP o FQDN del controlador de dominio principal. Se recomienda usar el FQDN para compatibilidad con Kerberos. No obstante, es incompatible con los modos de implementación SaaS-VPN, que deben usar la dirección IP en su lugar.

Puerto de LDAP
Puerto de LDAP del controlador de dominio principal

Puerto del catálogo global
Puerto del catálogo global del controlador de dominio principal

Puerto de SMB
Puerto de SMB del controlador de dominio principal

4. En la sección **Información principal**, escriba la siguiente información:

- En el cuadro **Nombre**, escriba el nombre del dominio.
- En el cuadro **FQDN del dominio**, escriba el nombre de dominio completo (FQDN) para el dominio.
- En el cuadro desplegable **Bosque**, seleccione el bosque al que pertenece el dominio.

5. **Análisis con privilegios** (opcional): si habilita el conmutador, permitirá que la cuenta "dcadmin" en este bosque recopile datos privilegiados de este dominio para hacer un análisis de seguridad avanzado.



6. **Transferencia de análisis con privilegios:** para obtener más información sobre esta opción, consulte [Recopilación de datos de Tenable Cloud](#).

7. En la sección **Controlador de dominio principal**, escriba la siguiente información:

- En el cuadro **Dirección IP o nombre de host**, escriba el nombre de host del controlador de dominio principal (obligatorio para la compatibilidad con [Autenticación de Kerberos](#), pero incompatible con los modos de implementación de SaaS-VPN) o la dirección IP.

Tenable Identity Exposure no admite equilibradores de carga.

- En el cuadro **Puerto de LDAP**, escriba el puerto LDAP del controlador de dominio principal.

Nota: Si usa el puerto TCP/636 (LDAPS) para conectarse al dominio, Tenable Identity Exposure debe tener acceso al certificado de la autoridad de certificación (CA) de Active Directory para validar el certificado de AD con el fin de establecer la conexión. En entornos de Secure Relay, puede instalar el certificado de la CA en la máquina de Relay. En entornos de VPN, esta configuración no es posible.

- En el cuadro **Puerto del catálogo global**, escriba el puerto del catálogo global del controlador de dominio principal.
- En el cuadro **Puerto de SMB**, escriba el puerto de SMB del controlador de dominio principal.


8. Haga clic en **Agregar**.

Aparece un mensaje para confirmar que Tenable Identity Exposure agregó el dominio.

Para editar un dominio:

1. En Tenable Identity Exposure, haga clic en **Sistema**.
2. Haga clic en la pestaña **Gestión de dominios**.

Aparece el panel **Gestión de dominios**.

3. Pase el cursor por el nombre del dominio que quiere editar para mostrar el ícono  a la derecha.



4. Haga clic en el ícono .

Aparece el panel **Editar un dominio**.

5. Edite la información del dominio.

6. Haga clic en **Editar**.


Aparece un mensaje para confirmar que Tenable Identity Exposure actualizó el dominio.

Para eliminar un dominio y los datos históricos:

1. En Tenable Identity Exposure, haga clic en **Sistema**.

2. Haga clic en la pestaña **Gestión de dominios**.

Aparece el panel **Gestión de dominios**.

3. Pase el cursor por el nombre del dominio que quiere eliminar para mostrar el ícono .

4. Haga clic en el ícono .

Aparece un mensaje para pedirle que confirme la eliminación del dominio "nombre_de_dominio".

5. Haga clic en **Eliminar**.

Aparece un mensaje para confirmar que Tenable Identity Exposure eliminó el dominio.

6. Espere a que el sistema limpie todos los datos históricos de Active Directory asociados al dominio eliminado.

Consulte también

- [Forzar la actualización de datos en un dominio](#)
- [Cuentas honey](#)
- [Autenticación de Kerberos](#)



Forzar la actualización de datos en un dominio



Para forzar la actualización de datos en un dominio:

1. En Tenable Identity Exposure, haga clic en **Sistema**.
2. Haga clic en la pestaña **Gestión de dominios**.

Aparece el panel **Gestión de dominios**.

3. Pase el cursor por el nombre del dominio en el que quiere forzar la actualización de datos para mostrar el ícono  a la derecha.
4. Haga clic en el ícono .

Aparece un mensaje con información sobre la acción de actualización de los datos.

5. Haga clic en **Confirmar**.

Consulte también

- [Cuentas honey](#)

Cuentas honey

Rol de usuario obligatorio: administrador en la máquina local

Una cuenta honey es una cuenta señuelo cuyo único fin es detectar a un atacante que intenta poner en riesgo la red a través de la instancia de Active Directory.

Es requisito previo que la funcionalidad de indicadores de ataque de Tenable Identity Exposure detecte intentos de explotación de Kerberoasting que buscan obtener acceso a cuentas de servicio mediante la solicitud y extracción de tickets de servicio para luego descifrar las credenciales de la cuenta de servicio sin conexión. El indicador de ataque Kerberoasting envía alertas cuando la cuenta honey recibe intentos de inicio de sesión o solicitudes de tickets.

Se asocia una cuenta honey por dominio. Las cuentas honey no se relacionan con los perfiles de seguridad.

Para agregar una cuenta honey:



1. En Tenable Identity Exposure, haga clic en **Sistema > Gestión de dominios**.


Aparece el panel **Gestión de dominios**.


2. Pase el cursor por el dominio para el que quiere agregar una cuenta honey.
3. Bajo **Estado de configuración de la cuenta honey**, haga clic en **+**.


Aparece el panel **Agregar una cuenta honey**.

4. En el cuadro **Nombre**, escriba un nombre distintivo (DN) para la cuenta de usuario que se usará como cuenta honey.

Sugerencia: Puede escribir cualquier cadena para que Tenable Identity Exposure busque y muestre los nombres de las cuentas de usuario coincidentes en el cuadro desplegable si esa cuenta de usuario ya existe en Active Directory.

5. En la sección **Implementación**, Tenable Identity Exposure genera un script con las opciones adecuadas para que lo ejecute para implementar la cuenta honey. Haga clic en  para copiar este script.
6. Haga clic en **Agregar**.

Aparece un mensaje para confirmar que Tenable Identity Exposure agregó la cuenta honey. En el panel "Gestión de dominios", el valor de **Estado de configuración de la cuenta honey** del dominio seleccionado aparece en naranja () para indicar que tiene que ejecutar el script de implementación de la cuenta honey para activarla.

Nota: Si el valor de **Estado de configuración de la cuenta honey** aparece en rojo () , es señal de que Tenable Identity Exposure no encontró esta cuenta de usuario en Active Directory. Tiene que crear esta cuenta de usuario y continuar con el siguiente paso.

7. En Windows PowerShell, en una máquina con el módulo de Active Directory, ejecute el script de implementación de la cuenta honey que copió.

En el panel **Gestión de dominios**, el valor de **Estado de configuración de la cuenta honey** del dominio seleccionado aparece con un estado verde () para indicar que está activa.

Nota: Tenable Identity Exposure puede tardar algún tiempo en procesar y activar la cuenta honey.



Para editar una cuenta honey:

1. En Tenable Identity Exposure, haga clic en **Sistema > Gestión de dominios**.

Aparece el panel **Gestión de dominios**.

2. Pase el cursor por el dominio para el que quiere agregar una cuenta honey.


3. En **Estado de configuración de la cuenta honey**, haga clic en el ícono  a la derecha.


Aparece el panel **Editar una cuenta honey**.

4. En el cuadro **Nombre**, modifique la cuenta de usuario según sea necesario.

5. En la sección **Implementación**, haga clic en  para copiar el script de implementación de la cuenta honey.

6. Haga clic en **Editar**.

Aparece un mensaje para confirmar que Tenable Identity Exposure actualizó la cuenta honey. En el panel "Gestión de dominios", el valor de **Estado de configuración de la cuenta honey** del dominio seleccionado aparece en naranja () para indicar que tiene que ejecutar el script de implementación de la cuenta honey para activarla.

Nota: Si el valor de **Estado de configuración de la cuenta honey** aparece en rojo () , es señal de que Tenable Identity Exposure no encontró esta cuenta de usuario en Active Directory. Tiene que crear esta cuenta de usuario y continuar con el siguiente paso.

7. En Windows PowerShell, en una máquina con el módulo de Active Directory, ejecute el script de implementación de la cuenta honey que copió.

En el panel **Gestión de dominios**, el valor de **Estado de configuración de la cuenta honey** del dominio seleccionado aparece con un estado verde () para indicar que está configurada.

Nota: Tenable Identity Exposure puede tardar algún tiempo en procesar y activar la cuenta honey.

Para eliminar una cuenta honey:



1. En Tenable Identity Exposure, haga clic en **Sistema > Gestión de dominios**.

Aparece el panel **Gestión de dominios**.

2. Pase el cursor por el dominio para el que quiere agregar una cuenta honey.

3. En **Estado de configuración de la cuenta honey**, haga clic en el ícono  a la derecha.

Aparece el panel **Editar una cuenta honey**.

4. Haga clic en **Eliminar**.

Aparece un mensaje para confirmar que Tenable Identity Exposure eliminó la cuenta honey.

Consulte también

- [Forzar la actualización de datos en un dominio](#)

Autenticación de Kerberos

Tenable Identity Exposure se autentica en los controladores de dominio configurados mediante las credenciales que usted proporcionó. Estos controladores de dominio aceptan la autenticación de NTLM o Kerberos. NTLM es un protocolo heredado con problemas de seguridad documentados, por lo que ahora Microsoft y todos los estándares de ciberseguridad desaconsejan su uso. Por otro lado, Kerberos es un protocolo más sólido que debería tenerse en cuenta. Windows siempre lo intenta primero con Kerberos y recurre a NTLM únicamente si Kerberos no está disponible.

Tenable Identity Exposure es compatible tanto con NTLM como con Kerberos, con algunas excepciones. Tenable Identity Exposure prioriza Kerberos como protocolo preferido cuando cumple con todas las condiciones necesarias. En esta sección se describen los requisitos y se muestra cómo configurar Tenable Identity Exposure para garantizar el uso de Kerberos.

El uso de NTLM en lugar de Kerberos también es el motivo por el que el endurecimiento de SYSVOL interfiere con Tenable Identity Exposure. Para obtener más información, consulte [Interferencia de endurecimiento de SYSVOL con Tenable Identity Exposure](#).

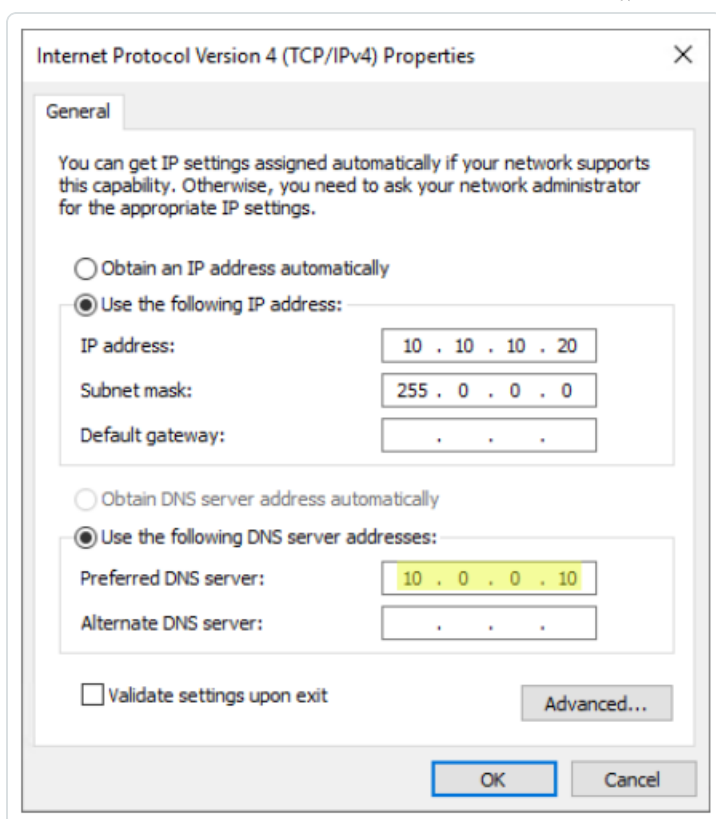
Compatibilidad con los modos de implementación de Tenable Identity Exposure



Modo de implementación	Compatibilidad con Kerberos
En el entorno local	Sí
SaaS-TLS (heredado)	Sí
SaaS con Secure Relay de Tenable Identity Exposure	Sí
SaaS con VPN	No, tiene que cambiar la instalación al modo de implementación de Secure Relay de Tenable Identity Exposure .

Requisitos técnicos

- **La cuenta de servicio de AD configurada en Tenable Identity Exposure debe tener un UserPrincipalName (UPN).** Para obtener instrucciones, consulte [Configuración de la cuenta de servicio y del dominio](#).
- **La configuración de DNS y el servidor DNS deben permitir resolver todas las entradas de DNS necesarias:** tiene que configurar la máquina de Directory Listener o Relay para que use servidores DNS que conozcan los controladores de dominio. Si la máquina de Directory Listener o Relay está unida a un dominio, [lo que Tenable Identity Exposure no recomienda](#), ya debería cumplir con este requisito. La manera más sencilla es usar el propio controlador de dominio como servidor DNS preferido, dado que normalmente también ejecuta DNS. Por ejemplo:



Nota: Si la máquina de Directory Listener o Relay está conectada a varios dominios y, potencialmente, a varios bosques, asegúrese de que los servidores DNS configurados puedan resolver todas las entradas DNS necesarias para todos los dominios. De lo contrario, tendrá que configurar varias máquinas de Directory Listener o Relay.

- **Accesibilidad del "servidor" de Kerberos (KDC):** requiere conectividad de red desde Directory Listener o Relay a los controladores de dominio a través del puerto TCP/88. Si Directory Listener o Relay están unidos a un dominio, [lo que Tenable no recomienda](#), ya debería cumplir con este requisito. Cada bosque de Tenable Identity Exposure configurado requiere conectividad de red Kerberos con al menos un controlador de dominio en su dominio correspondiente que contenga la cuenta de servicio, así como al menos un controlador de dominio en cada dominio conectado.

Para obtener más información sobre los requisitos, consulte [Matriz de flujos de red](#).

Nota: La máquina de Directory Listener o Relay no necesita estar unida a un dominio para usar Kerberos.

Configuración de la cuenta de servicio y del dominio



Para configurar la cuenta de servicio de AD y el dominio de AD en Tenable Identity Exposure para que usen Kerberos:

1. Use el formato de UserPrincipalName (UPN) para iniciar sesión. En este ejemplo, el atributo UPN es "tenablead@lab.1an".
 - a. Ubique el atributo UPN en el dominio del bosque que contiene la cuenta de servicio de la siguiente manera:

tenablead Properties

Published Certificates	Member Of	Password Replication	Dial-in	Object	
Security	Environment	Sessions	Remote control		
Remote Desktop Services Profile	COM+	Attribute Editor			
General	Address	Account	Profile	Telephones	Organization

User logon name:
tenablead @lab.1an

User logon name (pre-Windows 2000):
LAB\ tenablead

Logon Hours... Log On To...

Unlock account

```
PS C:\Users\admin> Get-ADUser tenablead

DistinguishedName : CN=tenablead,CN=Users,DC=lab,DC=1an
Enabled           : True
GivenName        : tenablead
Name             : tenablead
ObjectClass      : user
ObjectGUID       : 70020328-b176-40d0-8a79-7948c1d4cb74
SamAccountName   : tenablead
SID              : S-1-5-21-1891480667-311803191-3341389180-22602
Surname          :
UserPrincipalName : tenablead@lab.1an
```

Nota: El UPN parece una dirección de correo electrónico, e incluso a menudo (aunque no siempre) es el mismo que el correo electrónico del usuario.



- b. En Tenable Identity Exposure, en la sección de configuración del bosque, defina este UPN en lugar del formato corto "nombre de usuario" o el formato de NetBIOS "dominio\nombre de usuario", de la siguiente manera:

The screenshot shows the 'Gestión de bosques' interface in Tenable Identity Exposure. The main window is titled 'Editar un bosque'. On the left, a sidebar lists 9 objects with a search bar. The main content area is divided into two sections: 'INFORMACIÓN PRINCIPAL' and 'CUENTA'. Under 'INFORMACIÓN PRINCIPAL', the 'Nombre*' field contains 'ALSID.CORP Forest (prod)'. Under 'CUENTA', the 'Nombre de usuario*' field contains 'svc.alsid@alsid.corp'. Below this field, there is explanatory text: 'Inicio de sesión de la cuenta que usa Tenable.ad. Formato: nombre principal de usuario, como |tenablead@dominio.ejemplo.com (se recomienda para la compatibilidad con Kerberos); o NetBIOS como NombreDominioNetBIOS\NombreCuentaSam'. The 'Contraseña' field is currently empty and masked with dots. A note below it says 'Escriba una contraseña nueva solo si quiere cambiarla'.

2. Utilice el nombre de dominio completo (FQDN). En la configuración del dominio en Tenable Identity Exposure, defina el FQDN para el controlador de dominio principal (PDC) en lugar de su

IP.

Gestión de dominios Editar un dominio X

Gestión de re

INFORMACIÓN PRINCIPAL

Buscar

5 objetos

Nombre

ALSID

Japan Domai

KHLAB

TCORP Dom

TKJV4U

Nombre*

ALSID

Nombre del dominio

FQDN del dominio*

alsid.corp

Ejemplo: dominio.local

Bosque*

ALSID.CORP Forest (prod)

Bosque al que pertenece este dominio

Retransmisión*

TOOLS-ALSID

Retransmisión a la que pertenece este dominio

Análisis con privilegios

Al activar esta característica, indica que la cuenta `svc.alsid@alsid.corp` establecida en este bosque puede recopilar datos con privilegios de este dominio, como hashes de contraseñas. Estos datos se usarán para realizar análisis de seguridad adicionales. Esto es opcional. ⓘ

Transferencia de análisis con privilegios

Eligió transferir los datos con privilegios al servicio de Tenable Cloud. Puede cambiar esta opción para todos los dominios en [Configuración de Tenable Cloud](#).

CONTROLADOR DE DOMINIO PRINCIPAL

Dirección IP o FQDN*

apjlab-dc.alsid.corp

Dirección IP o FQDN del controlador de dominio principal. Se recomienda

Cancelar

Solucionar problemas

Para funcionar correctamente, Kerberos requiere varios pasos de configuración. De lo contrario, Windows y, por extensión, Tenable Identity Exposure, recurren silenciosamente a la autenticación de NTLM.

DNS

Asegúrese de que los servidores DNS usados en la máquina de Directory Listener o Relay puedan resolver el FQDN del PDC proporcionado, por ejemplo:



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Resolve-DnsName dc.lab.lan

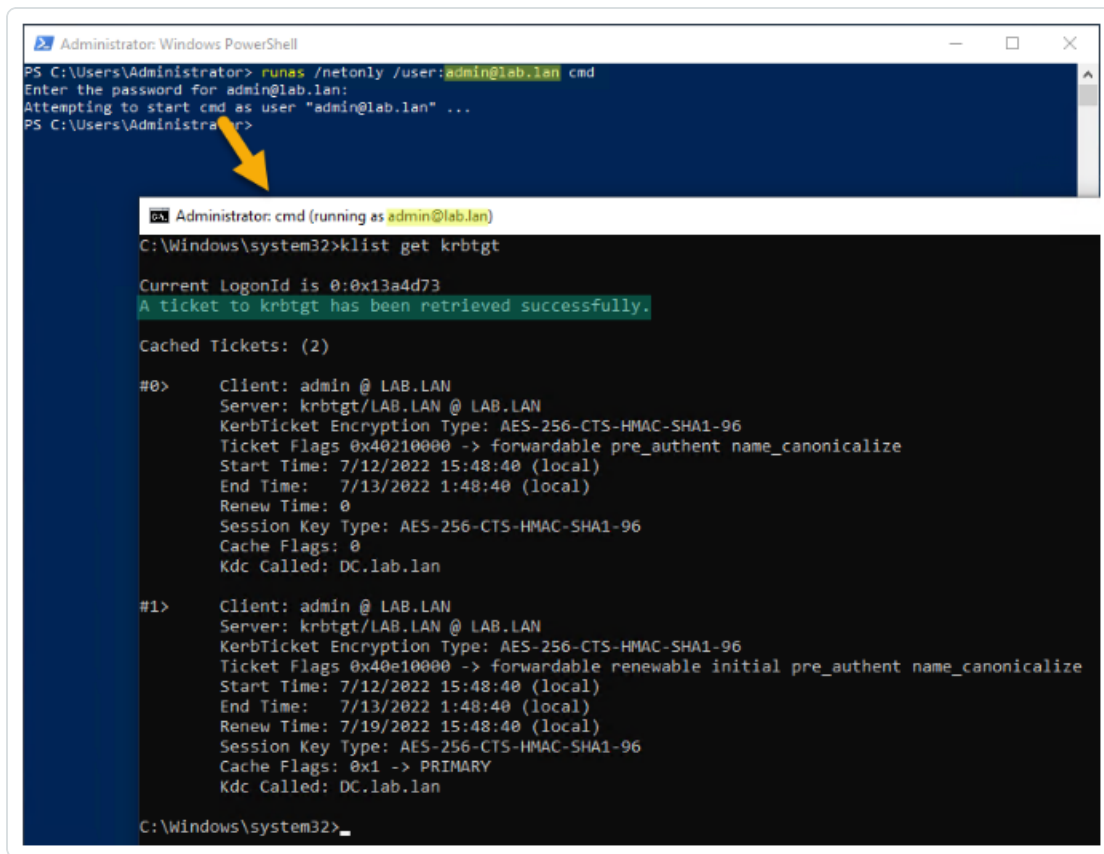
Name                Type      TTL      Section  IPAddress
----                -
dc.lab.lan          A         1200    Answer   10.0.0.10
```

Kerberos

Para verificar que Kerberos funcione con los comandos que ejecuta en la máquina de Directory Listener o Relay:

1. Verifique que la cuenta de servicio de AD configurada en Tenable Identity Exposure pueda obtener un TGT:
 - a. En una línea de comandos o PowerShell, ejecute "runas /netonly /user:<UPN> cmd " y escriba la contraseña. Tenga mucho cuidado al escribir o pegar la contraseña, ya que no hay verificación debido al indicador "/netonly".
 - b. En el segundo símbolo del sistema, ejecute "klist get krbtgt" para solicitar un ticket TGT.

En el siguiente ejemplo se muestra un resultado correcto:



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> runas /netonly /user:admin@lab.lan cmd
Enter the password for admin@lab.lan:
Attempting to start cmd as user "admin@lab.lan" ...
PS C:\Users\Administrator>

Administrator: cmd (running as admin@lab.lan)
C:\Windows\system32>klist get krbtgt

Current LogonId is 0:0x13a4d73
A ticket to krbtgt has been retrieved successfully.

Cached Tickets: (2)

#0> Client: admin @ LAB.LAN
Server: krbtgt/LAB.LAN @ LAB.LAN
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40210000 -> forwardable pre_authent name_canonicalize
Start Time: 7/12/2022 15:48:40 (local)
End Time: 7/13/2022 1:48:40 (local)
Renew Time: 0
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: DC.lab.lan

#1> Client: admin @ LAB.LAN
Server: krbtgt/LAB.LAN @ LAB.LAN
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 7/12/2022 15:48:40 (local)
End Time: 7/13/2022 1:48:40 (local)
Renew Time: 7/19/2022 15:48:40 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called: DC.lab.lan

C:\Windows\system32>
```

Los siguientes son posibles códigos de error:

- 0xc0000064: "User logon with misspelled or bad user account" -> Compruebe el nombre de usuario (es decir, la parte antes del "@" en el UPN).
- 0xc000006a: "User logon with misspelled or bad password" -> Compruebe la contraseña.
- 0xc000005e: "There are currently no logon servers available to service the logon request" -> Compruebe que la resolución de DNS funcione y que el servidor pueda comunicarse con los KDC devueltos, etc.
- Otros códigos de error: consulte la [documentación de Microsoft relacionada con los eventos 4625](#).

2. Verifique que el controlador de dominio configurado en Tenable Identity Exposure pueda obtener un ticket de servicio. En el mismo segundo símbolo del sistema, ejecute "klist get host/<FQDN_DC>" (reemplace "<FQDN_DC>").



En el siguiente ejemplo se muestra un resultado correcto:

```
Administrator: cmd (running as admin@lab.lan)
C:\Windows\system32>klist get host/dc.lab.lan

Current LogonId is 0:0x1434837
A ticket to host/dc.lab.lan has been retrieved successfully.

Cached Tickets: (3)

#0> Client: admin @ LAB.LAN
      Kdc Called: DC.lab.lan

#2> Client: admin @ LAB.LAN
      Server: host/dc.lab.lan @ LAB.LAN
      KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
      Ticket Flags 0x40250000 -> forwardable pre_authent ok_as_delegate name_canonicalize
      Start Time: 7/12/2022 15:55:00 (local)
      End Time: 7/13/2022 1:55:00 (local)
      Renew Time: 0
      Session Key Type: AES-256-CTS-HMAC-SHA1-96
      Cache Flags: 0
      Kdc Called: DC.lab.lan
```

Alertas

Licencia necesaria: según el tipo de alerta que quiera enviar, es posible que necesite licencias para indicadores de ataque o indicadores de exposición.

El sistema de alertas de Tenable Identity Exposure lo ayuda a detectar regresiones de seguridad o ataques en su instancia de Active Directory supervisada. Envía datos de análisis sobre vulnerabilidades y ataques en tiempo real a través de notificaciones de correo electrónico o SYSLOG.

- [Configuración de servidores SMTP](#)
- [Alertas de correo electrónico](#)
- [Alertas de SYSLOG](#)
- [Detalles de alertas de SYSLOG y de correo electrónico](#)

Configuración de servidores SMTP

Tenable Identity Exposure requiere la configuración del Protocolo simple de transferencia de correo (SMTP) para enviar notificaciones de alerta.



Diferencias en la arquitectura de implementación

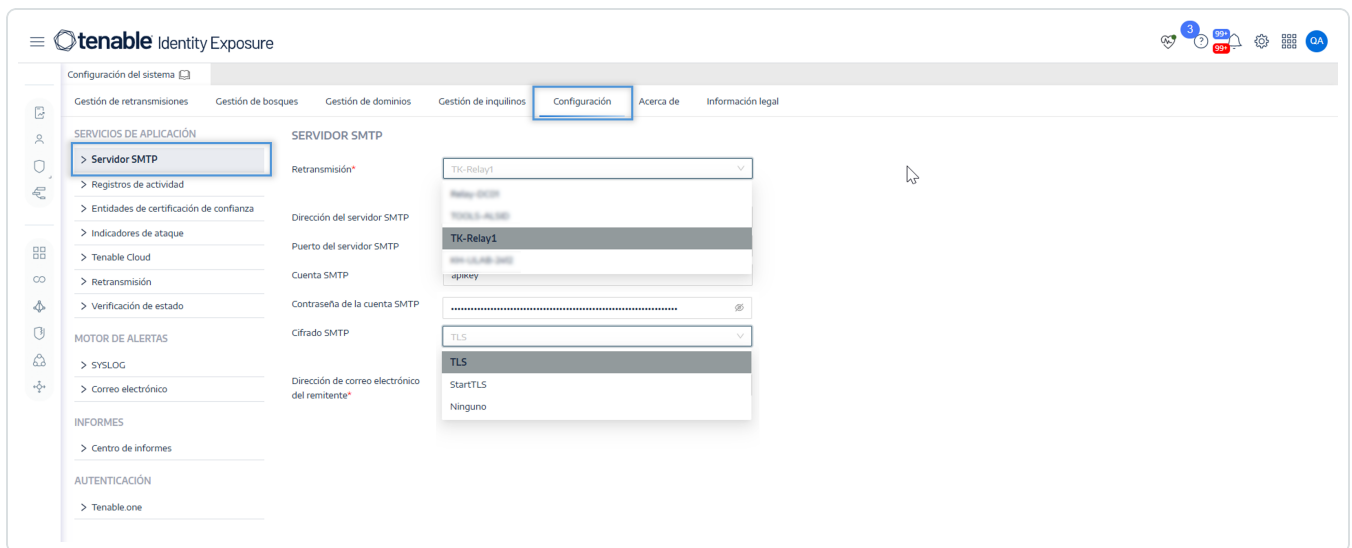
- Para la arquitectura de **Secure Relay**:
 - La instancia de Secure Relay se **instala en el entorno del cliente**.
 - Usted administra la comunicación entre Secure Relay y el servidor SMTP/SYSLOG.
- Para la arquitectura de **VPN**:
 - El servicio Secure Relay se **aloja en Tenable Cloud**.
 - Usted abre un caso de soporte en Tenable para administrar la comunicación de las alertas.

Configuración del servidor SMTP para entornos de Secure Relay

Para configurar el servidor SMTP **para Secure Relay**:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración**.
2. En **Servicios de aplicación**, seleccione **Servidor SMTP**.

Se abre el panel **Servidor SMTP**.



3. **Si la red usa Secure Relay**: en el cuadro **Relay**, haga clic en la flecha para seleccionar de la lista desplegable una instancia de Relay para que se comunique con el servidor SMTP.
4. Proporcione la siguiente información:



- Dirección del servidor SMTP
 - Puerto del servidor SMTP
 - Cuenta SMTP
 - Contraseña de la cuenta SMTP
5. En el cuadro “Cifrado SMTP”, haga clic en la flecha para seleccionar un método de cifrado de la lista desplegable.
 6. En el cuadro **Dirección de correo electrónico del remitente**, indique una dirección de correo electrónico para que Tenable Identity Exposure la use al enviar correos electrónicos.
 7. Haga clic en **Guardar**.

Un mensaje confirma que Tenable Identity Exposure actualizó los parámetros de SMTP.

Configuración del servidor SMTP para entornos de VPN

Para configurar el servidor SMTP **para VPN**:

1. Determine si el servidor SMTP se aloja:
 - **Dentro** de la red del cliente (**privado**).
 - **Fuera** de la red del cliente (**público**).
2. En función de la configuración de la red:
 - Para un servidor SMTP alojado **dentro** de la red del cliente:
 - Abra un caso de soporte para proporcionar la dirección IP privada del servidor SMTP a Tenable. Incluya la solicitud para permitir esta IP para la comunicación dentro del túnel VPN.
 - Espere a que el equipo de desarrollo de Tenable complete la configuración.
 - Pruebe el túnel VPN para confirmar la conectividad entre Tenable Cloud y el servidor SMTP interno.
 - Para un servidor SMTP alojado **fuera** de la red del cliente:
 - Confirme si el servidor SMTP externo filtra las conexiones entrantes:



- Si **se filtra** el tráfico entrante según la IP de origen:
 - Abra un caso de soporte en Tenable para solicitar la dirección IP de alertas para el túnel VPN.
 - Trabaje junto al proveedor SMTP externo para permitir la dirección IP de alertas de Tenable.
- Si **no se filtra** el tráfico entrante: asegúrese de que se pueda acceder a la IP pública del servidor SMTP a través del túnel VPN.

3. **Mantenimiento continuo:** para mantener la funcionalidad del túnel VPN, notifique a Tenable ante cualquier cambio en la dirección IP pública o privada del servidor SMTP.

Solución de problemas comunes

- **No se pueden enviar alertas (SMTP/SYSLOG):**
 - Verifique que se pueda acceder al servidor SMTP (privado o público) dentro del túnel VPN.
 - Confirme que la dirección IP se haya permitido en ambos extremos (Tenable Cloud y el servidor SMTP).
- **Se agotó el tiempo de espera de la conexión:**
 - Verifique la actividad del túnel VPN y la configuración de enrutamiento.

Alertas de correo electrónico

Tenable Identity Exposure envía alertas de correo electrónico para notificarle automáticamente si los eventos alcanzan un cierto umbral de gravedad y requieren acciones de corrección. El siguiente es un ejemplo de una alerta de correo electrónico:



This e-mail is best viewed in an HTML-capable mail-client.



A security incident (IOA) occurred on

You have received this email because you belong to Tenable.ad's alert notification list.

Technical details

- **Attack Name:** Golden Ticket
- **Description:** An adversary gains control over an Active Directory and uses that account to create valid Kerberos Ticket (TGTs).
- **Severity:** Critical
- **Timestamp:** 2020-12-07
- **Source:** CLIENT-HOST (10.2.37.15)
- **Target:** DC-01 (10.2.37.19)

Security considerations

The Indicator of Attack describes most of the time a major security incident on the monitored AD infrastructure. It is recommended to take quick incident response actions to qualify this risk.

[IoA details](#)

Para agregar una alerta de correo electrónico:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración > Correo electrónico**.
2. Haga clic en el botón **Agregar una alerta de correo electrónico** a la derecha.

Aparece el panel **Agregar una alerta de correo electrónico**.



3. En la sección **Información principal**, indique lo siguiente:
 - En el cuadro **Dirección de correo electrónico**, escriba la dirección de correo electrónico del destinatario para que reciba las notificaciones.
 - En el cuadro **Descripción**, escriba una descripción de la dirección del destinatario.
4. En la lista desplegable **Desencadenar la alerta**, seleccione una de las siguientes opciones:
 - **Con cada anomalía**: Tenable Identity Exposure envía una notificación tras cada detección de un loE anómalo.
 - **Con cada ataque**: Tenable Identity Exposure envía una notificación tras cada detección de un loA anómalo.
 - **Cuando cambia el estado de verificación de estado**: Tenable Identity Exposure envía una notificación cada vez que cambia el estado de una verificación de estado.
5. En el cuadro **Perfiles**, haga clic para seleccionar los perfiles que quiere usar para esta alerta de correo electrónico (si corresponde).
6. **Enviar alertas cuando se detecten anomalías durante la fase de análisis inicial**: siga uno de los procedimientos a continuación (si corresponde):
 - Seleccione la casilla: Tenable Identity Exposure envía un gran volumen de notificaciones de correo electrónico cuando un reinicio del sistema desencadena alertas.
 - Anule la selección de la casilla: Tenable Identity Exposure no envía notificaciones de correo electrónico cuando un reinicio del sistema desencadena alertas.
7. **Umbral de gravedad**: haga clic en la flecha del cuadro desplegable para seleccionar el umbral en el que Tenable Identity Exposure envía alertas (si corresponde).
8. Según el desencadenante de alertas que haya seleccionado anteriormente:
 - **Indicadores de exposición**: si configura alertas para que se desencadenen **con cada anomalía**, haga clic en la flecha junto a cada nivel de gravedad para expandir la lista de indicadores de exposición y seleccione aquellos para los cuales quiere enviar alertas.
 - **Indicadores de ataque**: si configura alertas para que se desencadenen **con cada ataque**, haga clic en la flecha junto a cada nivel de gravedad para expandir la lista de



indicadores de ataque y seleccione aquellos para los cuales quiere enviar alertas.

- **Cambios de estado de verificación de estado:** haga clic en **Verificaciones de estado** para seleccionar el tipo de verificación de estado que desencadenará una alerta y haga clic en **Filtrar selección**.

9. Haga clic en el cuadro **Dominios** para seleccionar los dominios para los que Tenable Identity Exposure envía alertas.

Aparece el panel "Bosques y dominios".

- a. Seleccione el bosque o el dominio.
- b. Haga clic en **Filtrar selección**.


10. Haga clic en **Probar la configuración**.

Un mensaje confirma que Tenable Identity Exposure envió una alerta de correo electrónico al servidor.

11. Haga clic en **Agregar**.

Un mensaje confirma que Tenable Identity Exposure creó la alerta de correo electrónico.

Para editar una alerta de correo electrónico:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración > Correo electrónico**.
2. En la lista de alertas de correo electrónico, pase el cursor por la que quiere modificar y haga clic en el ícono  al final de la línea.


Aparece el panel **Editar una alerta de correo electrónico**.

3. Haga las modificaciones necesarias según se describe en el procedimiento anterior ("[Para agregar una alerta de correo electrónico:](#)").
4. Haga clic en **Editar**.

Un mensaje confirma que Tenable Identity Exposure actualizó la alerta.

Para eliminar una alerta de correo electrónico:



1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración > Correo electrónico**.
2. En la lista de alertas de correo electrónico, pase el cursor por la que quiere eliminar y haga clic en el ícono  al final de la línea.

Aparece un mensaje para pedirle que confirme la eliminación.

3. Haga clic en **Eliminar**.

Un mensaje confirma que Tenable Identity Exposure eliminó la alerta.

Consulte también

- [Configuración de servidores SMTP](#)
- [Detalles de alertas de SYSLOG y de correo electrónico](#)

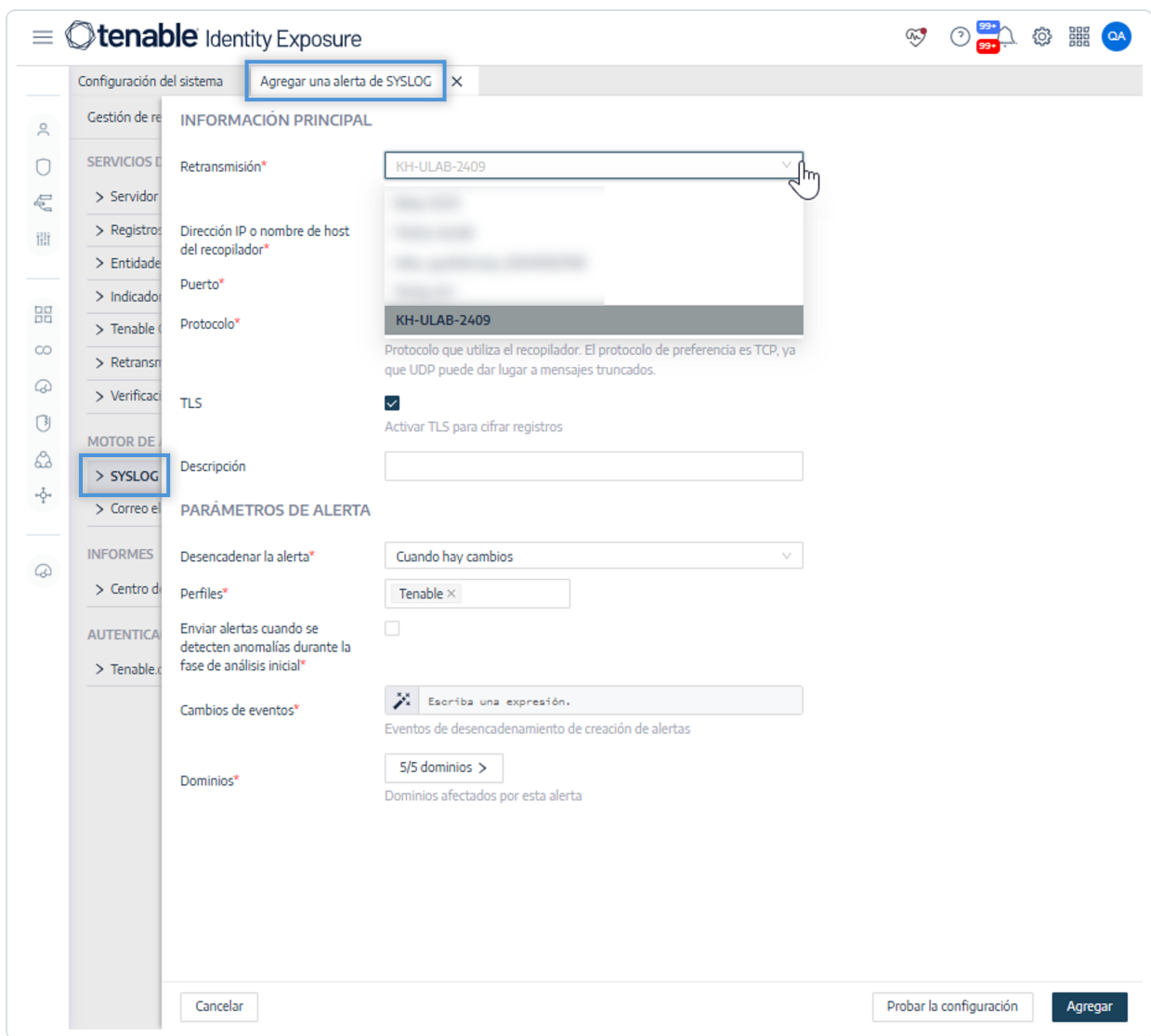
Alertas de SYSLOG

Algunas organizaciones utilizan SIEM (administración de eventos e información de seguridad) para recopilar registros sobre posibles amenazas e incidentes de seguridad. Tenable Identity Exposure puede enviar información de seguridad relacionada con Active Directory a los servidores SYSLOG de SIEM para mejorar los mecanismos de alerta.

Para agregar una nueva alerta de SYSLOG:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración > SYSLOG**.
2. Haga clic en el botón **Agregar una alerta de SYSLOG** a la derecha.

Aparece el panel **Agregar una alerta de SYSLOG**.



3. En la sección **Información principal**, indique lo siguiente:

- **Si la red usa Secure Relay:** en el cuadro **Relay**, haga clic en la flecha para seleccionar de la lista desplegable una instancia de Relay para que se comunique con la solución de SIEM.
- En el cuadro **Dirección IP o nombre de host del recopilador**, escriba la dirección IP o el nombre de host del servidor que recibe las notificaciones.
- En el cuadro **Puerto**, escriba el número de puerto del recopilador.
- En el cuadro **Protocolo**, haga clic en la flecha para seleccionar "UDP" o "TCP".



- Si elige "TCP", seleccione la casilla de la opción **TLS** si quiere habilitar el protocolo de seguridad TLS para cifrar los registros.
 - En el cuadro **Descripción**, escriba una descripción breve del recopilador.
4. En la lista desplegable **Desencadenar la alerta**, seleccione una opción:
- **Cuando hay cambios**: Tenable Identity Exposure envía una notificación cada vez que se produce un evento que se especificó.
 - **Con cada anomalía**: Tenable Identity Exposure envía una notificación tras cada detección de un loE anómalo.
 - **Con cada ataque**: Tenable Identity Exposure envía una notificación tras cada detección de un loA anómalo.
 - **Cuando cambia el estado de verificación de estado**: Tenable Identity Exposure envía una notificación cada vez que cambia el estado de una verificación de estado.
5. En el cuadro **Perfiles**, haga clic para seleccionar el perfil que quiere usar para esta alerta de SYSLOG (si corresponde).
6. **Enviar alertas cuando se detecten anomalías durante la fase de análisis inicial**: siga uno de los procedimientos a continuación (si corresponde):
- Seleccione la casilla: Tenable Identity Exposure envía un gran volumen de mensajes de SYSLOG cuando un reinicio del sistema desencadena alertas.
 - Anule la selección de la casilla: Tenable Identity Exposure no envía mensajes de SYSLOG cuando un reinicio del sistema desencadena alertas.
7. **Umbral de gravedad**: haga clic en la flecha del cuadro desplegable para seleccionar el umbral en el que Tenable Identity Exposure envía alertas (si corresponde).
8. Según el desencadenante de alertas que haya seleccionado anteriormente:
- **Cambios de eventos**: si configura las alertas para que se desencadenen **cuando hay cambios**, escriba una expresión para desencadenar la notificación del evento.
- Puede hacer clic en el ícono  para usar el asistente de búsqueda o escribir una expresión de consulta en el cuadro de búsqueda y hacer clic en **Validar**. Para obtener más información, consulte [Personalizar las consultas de Trail Flow](#).



- **Indicadores de exposición:** si configura alertas para que se desencadenen **con cada anomalía**, haga clic en la flecha junto a cada nivel de gravedad para expandir la lista de indicadores de exposición y seleccione aquellos para los cuales quiere enviar alertas.
 - **Indicadores de ataque:** si configura alertas para que se desencadenen **con cada ataque**, haga clic en la flecha junto a cada nivel de gravedad para expandir la lista de indicadores de ataque y seleccione aquellos para los cuales quiere enviar alertas.
 - **Cambios de estado de verificación de estado:** haga clic en **Verificaciones de estado** para seleccionar el tipo de verificación de estado que desencadenará una alerta y haga clic en **Filtrar selección**.
9. Haga clic en el cuadro **Dominios** para seleccionar los dominios para los que Tenable Identity Exposure envía alertas.

Aparece el panel **Bosques y dominios**.

- a. Seleccione el bosque o el dominio.
- b. Haga clic en **Filtrar selección**.


10. Haga clic en **Probar la configuración**.

Un mensaje confirma que Tenable Identity Exposure envió una alerta de SYSLOG al servidor.

11. Haga clic en **Agregar**.

Un mensaje confirma que Tenable Identity Exposure creó la alerta de SYSLOG.

Para editar una alerta de SYSLOG:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración > SYSLOG**.
2. En la lista de alertas de SYSLOG, pase el cursor por la que quiere modificar y haga clic en el ícono  al final de la línea.


Aparece el panel **Editar una alerta de SYSLOG**.

3. Haga las modificaciones necesarias según se describe en el procedimiento anterior ("[Para agregar una nueva alerta de SYSLOG:](#)").
4. Haga clic en **Editar**.



Un mensaje confirma que Tenable Identity Exposure actualizó la alerta.

Para eliminar una alerta de SYSLOG:

1. En Tenable Identity Exposure, haga clic en **Sistema > Configuración > SYSLOG**.
2. En la lista de alertas de SYSLOG, pase el cursor por la que quiere eliminar y haga clic en el ícono  al final de la línea.

Aparece un mensaje para pedirle que confirme la eliminación.

3. Haga clic en **Eliminar**.

Un mensaje confirma que Tenable Identity Exposure eliminó la alerta.

Consulte también

- [Detalles de alertas de SYSLOG y de correo electrónico](#)

Detalles de alertas de SYSLOG y de correo electrónico

Cuando habilita las alertas de SYSLOG o de correo electrónico, Tenable Identity Exposure envía notificaciones cuando detecta una anomalía, un ataque o un cambio.

Nota: Hay un tiempo de ingesta que se debe tener en cuenta antes de recibir alertas de IoA. Este retraso es diferente del que se observa durante la fase de “prueba de la configuración” cuando se configuran las alertas de SYSLOG y de correo electrónico. Por lo tanto, no utilice la duración de la configuración de prueba como referencia para comparar con el tiempo de las alertas que se desencadenan tras un ataque real.

Encabezado de alerta

Los encabezados de alertas de SYSLOG (RFC-3164) usan el formato de evento común (CEF), un formato común en soluciones que integran la administración de eventos e información de seguridad (SIEM).

Ejemplo de alerta para un indicador de exposición (IoE)



Encabezado de alerta de loE

```
<116>Jan 9 09:24:42 qradar.alsid.app AlsidForAD[4]: "0" "1" "Alsid Forest" "emea.corp" "C-PASSWORD-DONT-EXPIRE" "medium" "CN=Gustavo Fring,OU=Los_Pollos_Hermanos,OU=Emea,DC=emea,DC=corp" "28" "1" "R-DONT-EXPIRE-SET" "2434" "TrusteeCn"="Gustavo Fring"
```

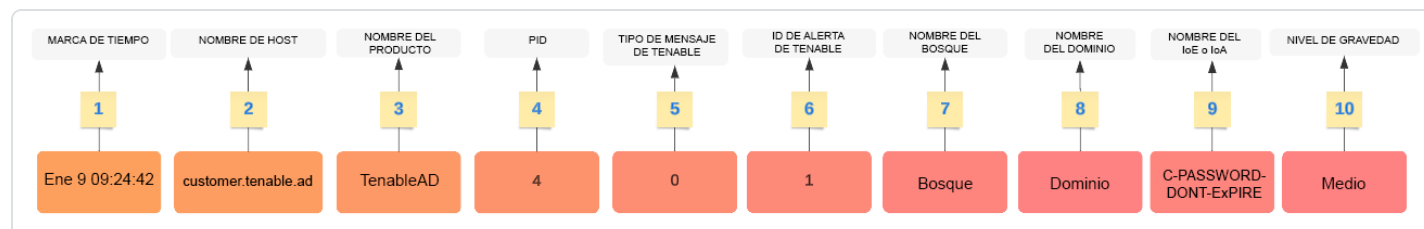
Ejemplo de alerta para un indicador de ataque (loA)

Encabezado de alerta de loA

```
<116>Jan 9 09:24:42 qradar.alsid.app AlsidForAD[4]: "2" "1337" "Alsid Forest" "emea.corp" "DC Sync" "medium" "yoda.alsid.corp" "10.0.0.1" "antoine1x.alsid.corp" "10.1.0.1" "user"="Gustavo Fring" "dc_name"="MyDC"
```

Información de la alerta

Elementos genéricos



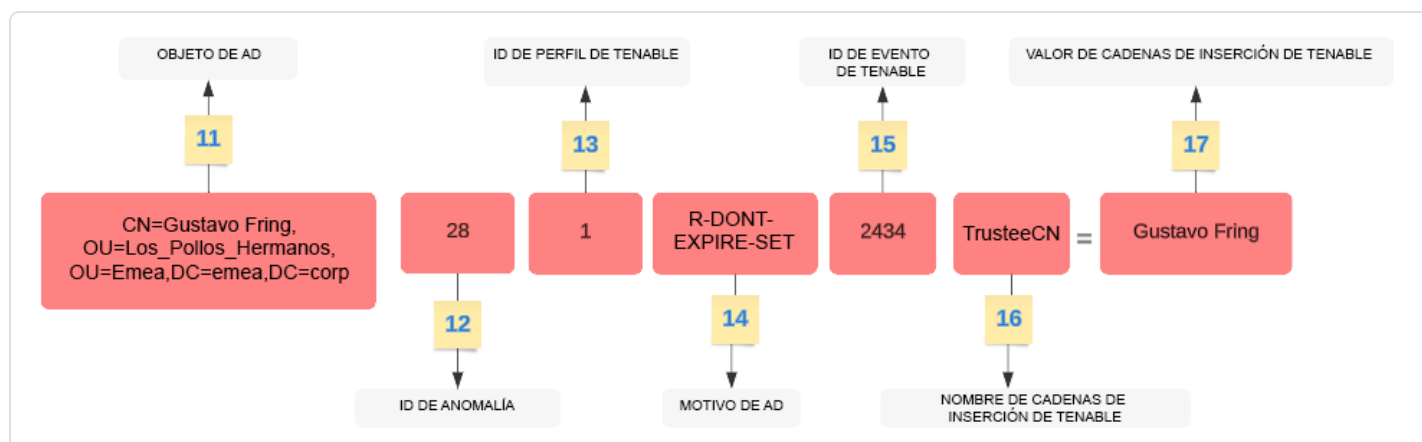
La estructura del encabezado incluye las siguientes partes, como se describe en la tabla.

Parte	Descripción
1	Marca de tiempo: fecha de la detección. Ejemplo: "Jun 7 05:37:03".
2	Nombre de host: nombre de host de la aplicación. Ejemplo: "cliente.tenable.ad".
3	Nombre del producto: nombre del producto que desencadenó la anomalía. Ejemplo: "TenableAD", "OtroProductoTenableAD".
4	PID: ID del producto (Tenable Identity Exposure). Ejemplo: [4].
5	Tipo de mensaje de Tenable: identificador de los orígenes de los eventos. Ejemplo: "0" (= Con cada anomalía), "1" (= Cuando hay cambios), "2" (= Con cada ataque), "3" (= Cuando cambia el estado de verificación de estado).
6	ID de alerta de Tenable: ID único de la alerta. Ejemplo: "0", "132".



7	Nombre del bosque: nombre del bosque del evento relacionado. Ejemplo: "Bosque corporativo".
8	Nombre del dominio: nombre de dominio relacionado con el evento. Ejemplo: "tenable.corp", "zwx.com".
9	Nombre en clave de Tenable: nombre en clave del indicador de exposición (IoE) o del indicador de ataque (IoA). Ejemplos: "C-PASSWORD-DONT-EXPIRE", "DC Sync".
10	Nivel de gravedad de Tenable: nivel de gravedad de la anomalía relacionada. Ejemplo: "crítica", "alta", "media".

Elementos específicos de los IoE

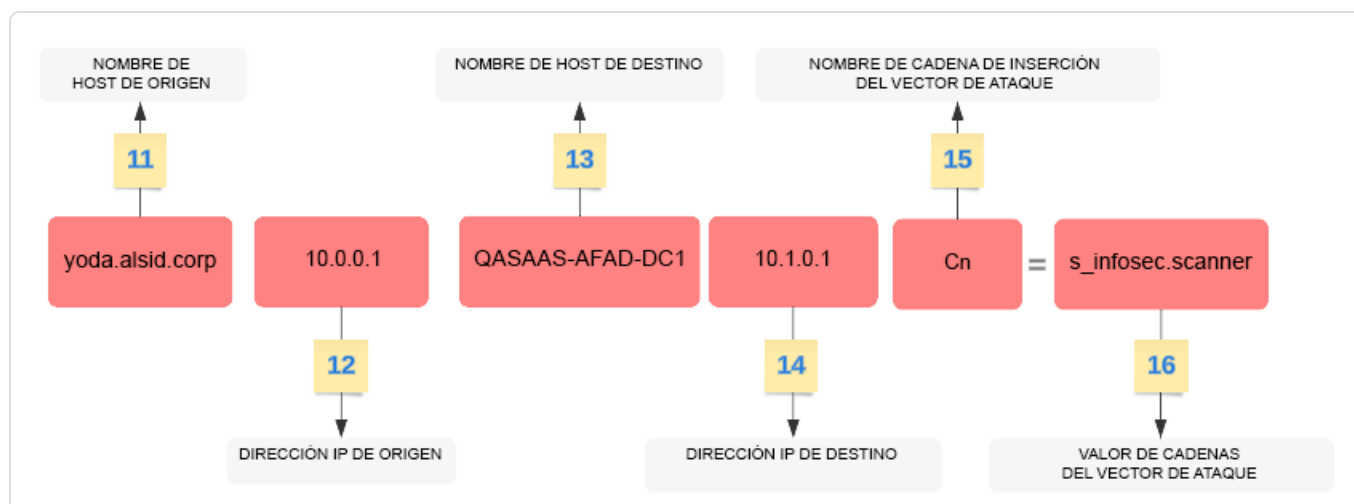


Parte	Descripción
11	Objeto de AD: nombre distintivo del objeto anómalo. Ejemplo: "CN=s_infosec.scanner,OU=ADManagers,DC=dominio,DC=local".
12	ID de anomalía de Tenable: ID de la anomalía. Ejemplo: "24980", "132", "28".
13	ID de perfil de Tenable: ID del perfil en el que Tenable Identity Exposure desencadenó la anomalía. Ejemplo: "1" (Tenable), "2" (sec_team).
14	Nombre en clave del motivo de AD: nombre en clave del motivo de la anomalía. Ejemplo: "R-DONT-EXPIRE-SET", "R-UNCONST-DELEG".
15	ID de evento de Tenable: ID del evento que la anomalía desencadenó. Ejemplo: "40667", "28".



16	Nombre de las cadenas de inserción de Tenable: nombre del atributo que desencadenó el objeto anómalo. Ejemplo: "Cn", "useraccountcontrol", "member", "pwdlastset".
17	Valor de las cadenas de inserción de Tenable: valor del atributo que desencadenó el objeto anómalo. Ejemplo: "s_infosec.scanner", "CN=Backup Operators,CN=Builtin,DC=domain,DC=local".

Elementos específicos de los loA



Parte	Descripción
11	Nombre de host de origen: nombre de host del host atacante. El valor también puede ser "Desconocido".
12	Dirección IP de origen: dirección IP del host atacante. Los valores pueden ser "IPv4" o "IPv6".
13	Nombre de host de destino: nombre de host del host atacado.
14	Dirección IP de destino: dirección IP del host atacado. Los valores pueden ser "IPv4" o "IPv6".
15	Nombre de las cadenas de inserción del vector de ataque: nombre del atributo que desencadenó el objeto anómalo.
16	Valor de las cadenas de inserción del vector de ataque: valor del atributo que desencadenó el objeto anómalo.



Marcos de mensajes de SYSLOG

- Para la configuración UDP y TCP de SYSLOG, Tenable Identity Exposure usa el método de marco no transparente según RFC-6587, sección 3.4.2 para delimitar los mensajes. El carácter de marco es el salto de línea (\n).
- Para TCP con TLS, Tenable Identity Exposure usa el método de conteo de octetos, como se describe en RFC-6587, sección 3.4.1.

Ejemplos

Detalles del evento de Trail Flow

En el siguiente ejemplo se muestran detalles de un evento en Trail Flow que contiene lo siguiente:

- La marca de tiempo (1)
- El nombre del objeto anómalo (11)
- Los nombres del bosque (7) y del dominio (8)
- El valor del atributo que desencadenó el objeto anómalo (17)

The screenshot shows the 'Detalles del evento' (Event Details) view in Trail Flow. The header contains the following information:

- ORIGEN: LDAP
- TIPO: UAC changed
- CLASE: user
- NOMBRE DE DOMINIO (11): CN=Kenneth Teo,CN=...
- DOMINIOS AFECTADOS (7): ALSID.CORP Forest (prod), Japan Domain @ Alsid corp (8)
- FECHA DEL EVENTO: 13:15:13, 2022-09-28

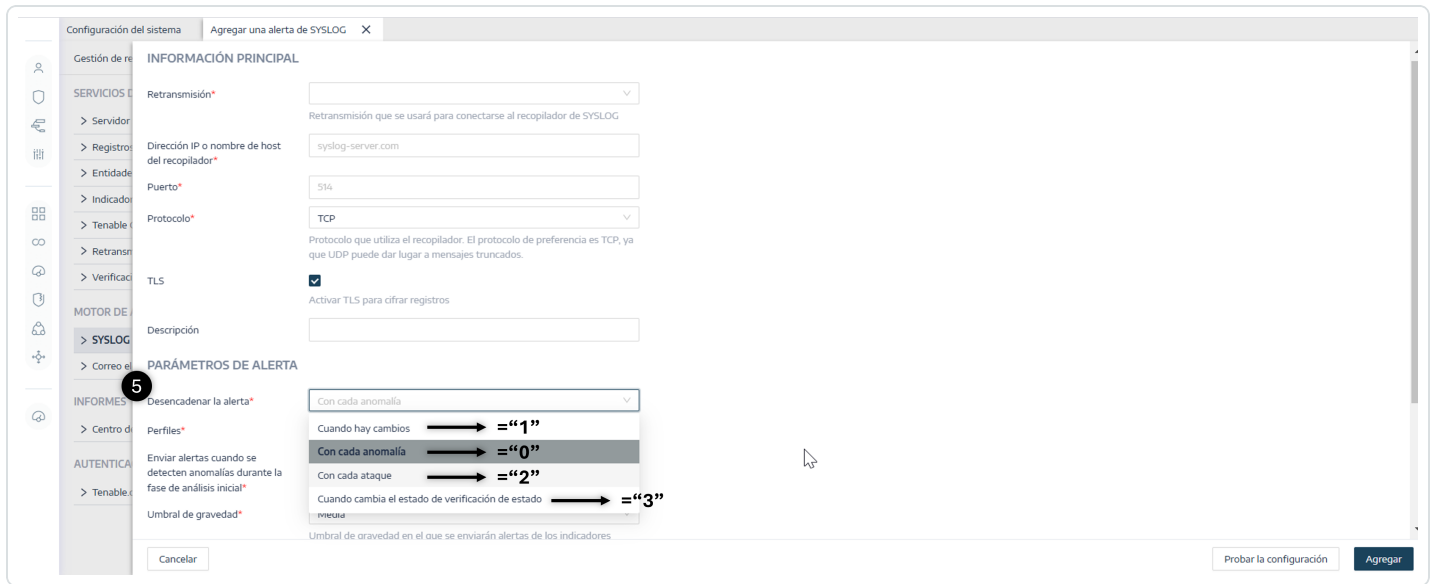
The main content area shows an 'Anomalías' (Anomalies) section with a card titled 'Sin obligación de cambiar la contraseña' (No password change requirement). The card contains the following text:

La cuenta de (17) kenneth Teo contiene el valor DONT_EXPIRE en su atributo userAccountControl, lo que excluye la cuenta de toda política de renovación de contraseñas. Además, ya que la cuenta no contiene ningún valor SMARTCARD_REQUIRED en el atributo dado, esto implica que no admite el uso de tarjetas inteligentes. Existe la posibilidad de que la cuenta de usuario use una contraseña vulnerable a ataques de fuerza bruta.

Below the card, there is a link: 'Cuentas con contraseñas que no vencen nunca'.

Origen del evento

En este ejemplo se muestra el origen del evento (5). Este parámetro se configura en la página de configuración de SYSLOG. Para obtener más información, consulte [Alertas de SYSLOG](#).



ID de alerta

En este ejemplo se muestra el ID único de la alerta (6), que se puede ver en la lista de direcciones de correo electrónico configuradas en **Sistema > Configuración > Correo electrónico** de Tenable Identity Exposure.



Verificaciones de estado

En este ejemplo se muestran los resultados de las verificaciones de estado que Tenable Identity Exposure realizó en su entorno. Para obtener más información, consulte [Verificaciones de estado](#).



i	Time	Event
>	3/5/25 6:57:56.000 AM	<109>Mar 5 06:57:56 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-DATA-COLLECTION" "SUCCESS" "TCORP Domain" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 6:57:54.000 AM	<109>Mar 5 06:57:54 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-REACHABILITY" "SUCCESS" "TCORP Domain" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 6:53:04.000 AM	<109>Mar 5 06:53:04 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-DATA-COLLECTION" "FAILURE" "TCORP Domain" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 6:53:04.000 AM	<109>Mar 5 06:53:04 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-REACHABILITY" "FAILURE" "TCORP Domain" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 3:18:00.000 AM	<109>Mar 5 03:18:00 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-PRIMARY-ROLE" "SUCCESS" "Japan Domain @ Alsid.corp" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 3:15:29.000 AM	<109>Mar 5 03:15:29 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-PRIMARY-ROLE" "SUCCESS" "ALSID" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 3:15:11.000 AM	<109>Mar 5 03:15:11 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-PRIMARY-ROLE" "FAILURE" "Japan Domain @ Alsid.corp" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 3:14:42.000 AM	<109>Mar 5 03:14:42 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-PRIMARY-ROLE" "FAILURE" "ALSID" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts
>	3/5/25 2:43:01.000 AM	<109>Mar 5 02:43:01 [redacted] Tenable.ad[4]: "3" "26" "HC-DOMAIN-REACHABILITY" "SUCCESS" "TKLab" host = [redacted] source = tcp:1338 sourcetype = tenable:ad:alerts

Verificaciones de estado

La funcionalidad de **verificación de estado** en Tenable Identity Exposure le proporciona visibilidad en tiempo real de la configuración de sus dominios y cuentas de servicio en una vista consolidada, desde la cual puede explorar en profundidad para investigar cualquier anomalía de configuración que provoque problemas de conectividad u otros problemas en la infraestructura. Verifica que todo esté configurado correctamente para garantizar el buen funcionamiento de Tenable Identity Exposure y le brinda la capacidad de tomar acciones rápidas y precisas para solucionar problemas, así como la confianza de que las opciones son las óptimas para permitir que Tenable Identity Exposure funcione de manera eficiente.

Las verificaciones de estado son visibles de manera predeterminada para los roles administrativos y con permiso para ciertos roles de usuario. También puede crear alertas de SYSLOG o de correo electrónico sobre cada cambio en el estado de la verificación de estado.

Verificaciones de estado y detección de ataques de sincronización de controladores de dominio

Las verificaciones de estado brindan información valiosa sobre el estado y la usabilidad de los servicios de Tenable Identity Exposure. Verifican la capacidad de la cuenta de servicio para recopilar información confidencial, como hashes de contraseñas y claves de copia de seguridad de



DPAPI usadas para Análisis con privilegios. En el informe de verificación de estado, Tenable intenta recopilar datos confidenciales para determinar si la cuenta de servicio tiene la funcionalidad Análisis con privilegios configurada correctamente, sin que se recopile nada en realidad si esta funcionalidad no está en uso. Para evitar la detección de un ataque DCSync durante este proceso, Tenable incluye automáticamente en la whitelist la cuenta de servicio proporcionada para el indicador de ataque DCSync.

Estado del dominio

Tenable Identity Exposure realiza las siguientes verificaciones para cada dominio:

- Autenticación en el dominio de AD: opciones y estado de LDAP, credenciales y acceso SMB.
- Accesibilidad del dominio: conexión funcional al puerto RPC dinámico, un servidor SMB accesible, un FQDN o una dirección IP de controlador de dominio accesible, una conexión funcional al puerto RPC, un servidor LDAP accesible y un servidor LDAP de catálogo global accesible.
- Permisos: capacidad de acceder a los datos del dominio de AD y recopilar datos privilegiados.
- Dominio vinculado a Relay: el dominio está asociado correctamente a un servicio de Relay.
- Indicadores de ataque: actividad de los controladores de dominio. Tenable Identity Exposure recibe los registros de eventos de Windows de todos los controladores de dominio.
- Indicadores de ataque: instalación de dominios. Asegúrese de que la configuración del GPO de loA de Tenable sea correcta.


Estado de la plataforma





Tenable Identity Exposure realiza las siguientes verificaciones en la configuración de la plataforma:

- Servicio de Relay en ejecución: si la configuración de Relay es correcta o no, con sugerencias para la solución de problemas.
- Coherencia de la versión de Relay: si la versión de Relay es coherente con la versión de Tenable Identity Exposure o no.
- Servicio de recopilación de datos de AD en ejecución: si el servicio de recopilación de datos, el agente y el puente de recopilación están operativos para retransmitir datos a otros servicios o no.



Para acceder a las verificaciones de estado:

1. En la esquina inferior izquierda de la página Tenable Identity Exposure, pase el cursor sobre el ícono  para ver el estado global de la infraestructura.
2. Haga clic en el ícono para abrir la página **Verificación de estado**. En la pestaña **Estado del dominio** o **Estado de la plataforma**, verá uno de los siguientes:
 - Un mensaje de que se superaron todas las verificaciones de estado.
 - Una lista de advertencias o problemas con estados específicos:


	La verificación se completó correctamente y muestra un resultado normal.
	La verificación falló y se identifica un problema.
	<p>La verificación falló, pero el problema no impide que Tenable Identity Exposure funcione correctamente.</p> <p>Por ejemplo, la verificación de la recopilación de datos generará un error debido a un error de configuración de Active Directory en el lado del cliente si la cuenta de servicio no puede recopilar datos privilegiados. Sin embargo, no es un problema grave, dado que no activó la funcionalidad Análisis con privilegios en este dominio en Tenable Identity Exposure, de ahí la advertencia. No obstante, si activa Análisis con privilegios, la verificación fallará de inmediato.</p>
	La verificación muestra un resultado desconocido porque una verificación dependiente falló. Por ejemplo, la verificación de accesibilidad de la red no puede continuar si falla la verificación de autenticación.

Para ver todas las verificaciones de estado:



- Sobre la lista de verificaciones de estado a la derecha, haga clic en el conmutador **Mostrar verificaciones correctas** para habilitarlo y enumerar todas las verificaciones que Tenable Identity Exposure realizó con la siguiente información:
 - Nombre de la verificación de estado
 - Estado (superada, no superada, no superada pero sin obstaculizar o desconocida)
 - Dominio afectado y su bosque asociado (solo para verificaciones del estado de dominios)
 - Hora de la última verificación realizada
 - Cuánto tiempo permaneció la verificación en este estado

Para actualizar la página "Verificación de estado":

- Aunque Tenable Identity Exposure realiza verificaciones de estado periódicamente, no actualiza la página con los resultados en tiempo real. Haga clic en  para actualizar la lista de resultados.

Para filtrar los resultados por tipo de verificación de estado o por dominio:

1. Sobre la lista de verificaciones de estado a la derecha, haga clic en **n/n verificaciones de estado** o **n/n dominios** (solo para el estado del dominio).
Se abre el panel **Verificaciones de estado** o **Bosques y dominios**.
2. Seleccione los tipos de verificación de estado o bosques o dominios (si corresponde) y haga clic en **Filtrar selección**.

Para obtener más información sobre cada verificación de estado:

1. En la lista de verificaciones de estado, haga clic en el nombre de una verificación o en la flecha azul (→) al final de la línea.
Se abre el panel **Detalles**, en el que se muestra una descripción de la verificación y una lista de detalles pertinentes. Para obtener más información, consulte [Lista de verificaciones de estado](#) a continuación.



2. Haga clic en la flecha al final de la línea de detalles para expandirla y mostrar más información sobre el resultado.

Para ocultar el ícono de estado de la verificación de estado:

De manera predeterminada, Tenable Identity Exposure muestra el ícono de estado de la verificación de estado en la esquina inferior izquierda de la pantalla.


1. En Tenable Identity Exposure, vaya a **Sistema** en la barra de navegación de la izquierda y seleccione la pestaña **Configuración**.

Como alternativa, puede hacer clic en  en la esquina superior derecha de la página "Verificación de estado" y seleccionar **Configuración**.

2. En **Servicios de aplicación**, seleccione **Verificación de estado**.
3. Haga clic en el conmutador **Mostrar el estado global de la verificación de estado** para deshabilitarlo.

Tenable Identity Exposure oculta el ícono de la verificación de estado en la esquina inferior izquierda de la pantalla.

Para asignar permisos de verificación de estado a los roles de usuario:

1. En Tenable Identity Exposure, vaya a **Cuentas** en la barra de navegación de la izquierda y seleccione la pestaña **Gestión de roles**.
2. En la lista de roles, seleccione el rol de usuario y haga clic en  al final de la línea.
Se abre el panel **Editar un rol**.
3. Seleccione la pestaña **Entidades de configuración del sistema**.
4. Seleccione la entidad **Verificación de estado** y haga clic en el conmutador de permiso para pasarlo de **Sin autorización** a **Concedido**.
5. Haga clic en **Aplicar y cerrar**.

Para obtener más información sobre los permisos, consulte [Establecer permisos para un rol](#).

Para configurar alertas para cambios en el estado de las verificaciones de estado:



1. En Tenable Identity Exposure, vaya a **Sistema** en la barra de navegación de la izquierda y seleccione la pestaña **Configuración**.

Como alternativa, puede hacer clic en  en la esquina superior derecha de la página "Verificación de estado" y seleccionar **Alertas**.

2. En **Motor de alertas**, seleccione **SYSLOG** o **Correo electrónico**.
3. Haga clic en **Agregar una alerta de SYSLOG** o **Agregar una alerta de correo electrónico**.
Se abre un nuevo panel. Para conocer el procedimiento completo, consulte [Alertas](#).
4. En **Parámetros de alerta**, en el cuadro **Desencadenar la alerta**, seleccione **Cuando cambia el estado de verificación de estado** en el menú desplegable.
5. Haga clic en la flecha en el cuadro **Verificaciones de estado** para seleccionar el tipo de verificación de estado que desencadenará una alerta y haga clic en **Filtrar selección**.
6. Haga clic en **Agregar**.

Lista de verificaciones de estado

Nombre de la verificación de estado	Tipo	Descripción de la verificación	Detalles
Accesibilidad al dominio (HC-DOMAIN-REACHABILITY)	Dominio	Capacidad para establecer una conexión con el dominio de AD	<ul style="list-style-type: none">• Dirección IP o FQDN del controlador de dominio accesible• Servidor LDAP del catálogo global accesible• Servidor LDAP accesible• Servidor SMB accesible• Conexión en



			<p>funcionamiento con el puerto RPC dinámico</p> <ul style="list-style-type: none">• Conexión en funcionamiento con el puerto RPC
<p>Autenticación en el dominio de AD (HC-DOMAIN-AUTHENTICATION)</p>	<p>Dominio</p>	<p>Capacidad para autenticarse en el dominio de AD</p>	<ul style="list-style-type: none">• Credenciales válidas• Servidor LDAP inactivo• Servidor LDAP disponible• Acceso LDAP concedido• Acceso SMB concedido
<p>Permisos para recopilar los datos de dominios de AD (HC-DOMAIN-DATA-COLLECTION)</p>	<p>Dominio</p>	<p>Capacidad para recopilar los datos de dominios de AD</p>	<ul style="list-style-type: none">• Permisos concedidos para recopilar datos con privilegios
<p>Permisos para acceder a los contenedores de AD (HC-DOMAIN-CONTAINER-ACCESS)</p>	<p>Dominio</p>	<p>Capacidad para acceder a los contenedores de AD</p>	<ul style="list-style-type: none">• Permisos concedidos para acceder al contenedor de objetos eliminados• Permisos concedidos para acceder al



			contenedor de configuración de contraseñas
Dominio vinculado a Relay (HC-DOMAIN-LINKED-TO-RELAY)	Dominio	El dominio está vinculado a una instancia de Relay	<ul style="list-style-type: none">• Dominio vinculado a una instancia de Relay
loA: actividad de los controladores de dominio	Dominio	Tenable Identity Exposure recibe los registros de eventos de Windows de todos los controladores de dominio	<ul style="list-style-type: none">• Controladores de dominio inactivos
loA: instalación de dominios	Dominio	Asegúrese de que la configuración del GPO de loA de Tenable sea correcta	<ul style="list-style-type: none">• El GPO de loA de Tenable existe en LDAP• La carpeta del GPO de loA de Tenable existe en SYSVOL• La carpeta de loA del GPO de loA de Tenable existe en SYSVOL• El archivo del cliente de escucha de suscripción de EVT del GPO de loA de Tenable existe en SYSVOL• El archivo de



			<p>configuración del GPO de loA de Tenable existe en SYSVOL</p> <ul style="list-style-type: none">• El archivo <code>audit.csv</code> del GPO de loA de Tenable existe en SYSVOL
Servicio Relay activo (HC-PLATFORM-RELAY-UP)	Plataforma	Relay funciona según lo esperado	<ul style="list-style-type: none">• Ejecución del servicio Relay
Versión del servicio Relay (HC-PLATFORM-RELAY-VERSION)	Plataforma	La versión de Relay es compatible con el producto	<ul style="list-style-type: none">• Coherencia de la versión de Relay
Recopilador de datos de AD activo (HC-PLATFORM-AD-DATA-COLLECTOR-UP)	Plataforma	El recopilador de datos de AD funciona según lo esperado	<ul style="list-style-type: none">• Puente del recopilador de datos de AD en ejecución• Servicio del recopilador de datos de AD en ejecución• Agente en ejecución
Sincronización entre los servicios de Tenable Cloud y Tenable Identity	Plataforma	El grupo, los permisos y los usuarios de Tenable Cloud creados se	<ul style="list-style-type: none">• Disponibilidad de Tenable Cloud



Exposure		sincronizan con la base de datos de Tenable Identity Exposure	
----------	--	---	--

Centro de informes

El **Centro de informes** en Tenable Identity Exposure proporciona una funcionalidad valiosa que le permite exportar datos importantes como informes a las partes interesadas clave dentro de una organización. El Centro de informes ofrece un medio para crear informes a partir de una lista predefinida, lo que garantiza un proceso eficiente y optimizado.

Ofrece las siguientes funciones:

- **Filtrado detallado:** ajuste los informes mediante filtros detallados basados en rangos de fechas, dominios, indicadores de ataque (IoA), indicadores de exposición (IoE) y más, lo que garantiza información muy precisa.
- **Entrega automatizada:** programe informes para su generación y entrega automáticas en los intervalos deseados, lo que agiliza los procesos de supervisión y generación de informes de seguridad.
- **Exportación flexible:** exporte informes en varios formatos, como CSV, para su posterior análisis, y compártalos mediante una clave de acceso a los informes o intégreles en flujos de trabajo de informes existentes.

Los administradores pueden crear distintos tipos de informes para distintos usuarios con plazos de informes flexibles de hasta un trimestre. La capacidad de compartir datos de identidad críticos desde Tenable Identity Exposure permite a la organización mitigar de forma proactiva los riesgos e identificar posibles ataques basados en la identidad.

Para descargar un informe, los usuarios reciben un correo electrónico con una dirección URL a una página en la que ingresan una clave de acceso al informe que recibieron del administrador. Los informes están disponibles para su descarga durante 30 días, después de los cuales vencen y Tenable Identity Exposure los elimina. Los usuarios deben descargar los informes antes de que Tenable Identity Exposure genere uno nuevo para el período de tiempo especificado y sobrescriba el anterior.



Para acceder al Centro de informes:

1. En Tenable Identity Exposure, seleccione **Sistema > Configuración**.
2. En **Informes**, haga clic en **Centro de informes**.

Se abre un panel con una lista de informes configurados y su información asociada, como el nombre del informe, el tipo, el dominio, el perfil, el período, la periodicidad y los correos electrónicos de los destinatarios.

Para crear un informe:

1. En el panel **Centro de informes**, haga clic en **Crear un informe**.

Se abre el panel **Configuración de informes**.

2. En **Tipo de informe**, complete la siguiente información:
 - a. En **Tipo de informe**, seleccione **Anomalías** o **Ataques**.
 - b. En **Indicadores**, haga clic en **n/n indicadores** para seleccionar **Indicadores de exposición** (para anomalías) o **Indicadores de ataque** (para ataques) y haga clic en **Filtrar selección**.
 - c. En **Dominios**, haga clic en **n/n dominios** para seleccionar los bosques o dominios para el informe y haga clic en **Filtrar selección**.
 - d. En **Perfiles**, haga clic en la flecha para seleccionar un perfil del menú desplegable.
3. En **Nombre del informe**, escriba un nombre para el informe.
4. En **Parámetros de generación**, seleccione las siguientes opciones:
 - a. **Período de tiempo de los datos**: el informe abarca el período anterior al actual, como el día, la semana, el mes o el trimestre anteriores.
 - b. **Periodicidad**: Tenable Identity Exposure genera un nuevo informe para cada período de tiempo que se defina. Haga clic en la flecha para seleccionar los valores correspondientes en el menú desplegable.
 - c. **Huso horario**: huso horario asociado al informe.





5. En **Destinatarios**, haga clic en **Agregar correos electrónicos** y escriba la dirección de correo electrónico del destinatario. Puede agregar tantos destinatarios como necesite.

Para obtener información sobre cómo configurar correos electrónicos para los destinatarios de los informes, consulte [Configuración de servidores SMTP](#).


6. Haga clic en **Crear informe**.

Para permitir que los usuarios descarguen un informe:


- En la parte superior del panel **Centro de informes**, en **Clave de acceso a los informes**, haga clic en  para copiarla. Esta clave de acceso es obligatoria para descargar el informe desde el vínculo incluido en el correo electrónico que se envía al destinatario. Es exclusiva para todos los usuarios e informes.
- Si es necesario, haga clic en  para generar una nueva clave de acceso.

Precaución: Generar una nueva clave de acceso hace que la anterior quede inservible. Solo la nueva clave de acceso puede conceder acceso a los informes existentes.

Para editar la configuración de un informe:

1. En la lista de informes, seleccione uno y haga clic en  al final de la línea para abrir el panel **Configuración de informes**.
2. Haga las modificaciones que considere necesarias.
3. Haga clic en **Guardar**.

Para eliminar un informe:

1. En la lista de informes, seleccione uno y haga clic en  al final de la línea para eliminarlo.
Aparece un mensaje para pedirle que confirme la eliminación.
2. Haga clic en **Eliminar**.

El informe generado más recientemente asociado a esta configuración de informes ya no está disponible para descargar.



Para otorgar permisos a los roles:

- En **Gestión de permisos**, en **Entidades de datos > Informes**, los administradores pueden otorgar permisos a los roles de usuario para crear, leer o editar todas las configuraciones de informes o algunas específicas.

Para obtener más información, consulte [Establecer permisos para un rol](#).

Compatibilidad con Microsoft Entra ID

Además de Active Directory, Tenable Identity Exposure admite Microsoft Entra ID (anteriormente, Azure AD o AAD) para ampliar el ámbito de las identidades en una organización. Esta funcionalidad aprovecha nuevos indicadores de exposición que se centran en los riesgos específicos de Microsoft Entra ID.

Para integrar Microsoft Entra ID en Tenable Identity Exposure, siga de cerca este proceso de incorporación:

1. Cumplir con los [Requisitos previos](#).
2. Comprobar los [Permisos](#).
3. [Configurar las opciones de Microsoft Entra ID](#)
4. [Activar la compatibilidad con Microsoft Entra ID](#)
5. [Habilitar escaneos de inquilinos](#)

Requisitos previos

Necesita una cuenta de Tenable Cloud para iniciar sesión en "cloud.tenable.com" y usar la funcionalidad de compatibilidad con Microsoft Entra ID. Esta cuenta de Tenable Cloud es la misma dirección de correo electrónico usada para el correo electrónico de bienvenida. Si no conoce su dirección de correo electrónico para "cloud.tenable.com", póngase en contacto con Soporte. Todos los clientes que tengan una licencia válida (local o SaaS) pueden acceder a Tenable Cloud en "cloud.tenable.com". Esta cuenta le permite configurar los escaneos de Tenable para su instancia de Microsoft Entra ID y recopilar los resultados de los escaneos.



Nota: No necesita una licencia de **Tenable Vulnerability Management** válida para acceder a Tenable Cloud, alcanza con una licencia de Tenable Identity Exposure (local o SaaS) independiente actualmente válida.

Permisos

La compatibilidad de Microsoft Entra ID requiere la recopilación de datos de Microsoft Entra ID, como usuarios, grupos, aplicaciones, entidades de servicio, roles, permisos, políticas, registros, etc. Recopila estos datos mediante Microsoft Graph API y las credenciales de la entidad de servicio siguiendo las recomendaciones de Microsoft.

- Debe iniciar sesión en Microsoft Entra ID como **usuario con permisos para conceder el consentimiento del administrador para todo el inquilino** en Microsoft Graph, que debe tener el rol de Administrador global o Administrador de roles privilegiados (o cualquier rol personalizado con los permisos adecuados), [según Microsoft](#).
- Para acceder a la configuración y a la visualización de datos de Microsoft Entra ID, su **rol de usuario de Tenable Identity Exposure** debe tener los permisos adecuados. Para obtener más información, consulte [Establecer permisos para un rol](#).

Configurar las opciones de Microsoft Entra ID

Siga los procedimientos a continuación (adaptados a partir de la documentación de Microsoft [Inicio rápido: Registro de una aplicación en la plataforma de identidad de Microsoft](#)) para configurar todas las opciones necesarias en Microsoft Entra ID.

1. **Crear una aplicación:**
 - a. En el portal de administración de Azure, abra la página [Registros de aplicaciones](#).
 - b. Haga clic en **+ Nuevo registro**.
 - c. Asigne un nombre a la aplicación (ejemplo: "Tenable Identity Collector"). Para las demás opciones, puede dejar los valores predeterminados tal como están.
 - d. Haga clic en **Registrar**.
 - e. En la página "Descripción general" de esta aplicación recién creada, anote el "Id. de la aplicación (cliente)" y el "Id. del directorio (inquilino)".



2. Agregar credenciales a la aplicación:

- En el portal de administración de Azure, abra la página [Registros de aplicaciones](#).
- Haga clic en la aplicación que creó.
- En el menú de la izquierda, haga clic en **Certificados y secretos**.
- Haga clic en **+ Nuevo secreto de cliente**.
- En el cuadro **Descripción**, asigne un nombre práctico a este secreto y un valor de **Vencimiento** que cumpla con sus políticas. Recuerde renovar este secreto cerca de su fecha de vencimiento.
- Guarde el valor secreto en una ubicación segura, ya que Azure solo lo muestra una vez y debe volver a crearlo si lo pierde.

3. Asignar permisos a la aplicación:

- En el portal de administración de Azure, abra la página [Registros de aplicaciones](#).
- Haga clic en la aplicación que creó.
- En el menú de la izquierda, haga clic en **Permisos de API**.
- Elimine el permiso `User.Read` existente:

Home > App registrations > Tenable Identity Collector

Tenable Identity Collector | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for t8qdy

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	Remove permission

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

- Haga clic en **+ Agregar un permiso**:

Home > App registrations > Tenable Identity Collector

Tenable Identity Collector | API permissions

Search << Refresh Got feedback?

Warning: You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Manage

- Overview
- Quickstart
- Integration assistant
- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for t8qdy

API / Permissions name	Type	Description	Admin consent requ...	Status
No permissions added				

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

f. Seleccione **Microsoft Graph**:

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Communication Services

Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Rights Management Services


Allow validated users to read and write protected content

g. Seleccione **Permisos de aplicación** (no "Permisos delegados").



Request API permissions

[← All APIs](#)

 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

h. Use la lista o la barra de búsqueda para buscar y seleccionar todos los permisos siguientes:

- AuditLog.Read.All
- Directory.Read.All
- IdentityProvider.Read.All
- Policy.Read.All
- Reports.Read.All
- RoleManagement.Read.All
- UserAuthenticationMethod.Read.All

i. Haga clic en **Agregar permisos**.

j. Haga clic en **Otorgar consentimiento de administrador a <nombre del inquilino>** y haga clic en **Sí** para confirmar:

Home > App registrations > Tenable Identity Collector

Tenable Identity Collector | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

⚠ You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for [redacted]

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				
AuditLog.Read.All	Application	Read all audit log data	Yes	⚠ Not granted for [redacted]
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for [redacted]
IdentityProvider.Read.All	Application	Read identity providers	Yes	⚠ Not granted for [redacted]
Policy.Read.All	Application	Read your organization's policies	Yes	⚠ Not granted for [redacted]
Reports.Read.All	Application	Read all usage reports	Yes	⚠ Not granted for [redacted]
RoleManagement.Read.All	Application	Read role management data for all RBAC providers	Yes	⚠ Not granted for [redacted]
UserAuthenticationMethod.Reac	Application	Read all users' authentication methods	Yes	⚠ Not granted for [redacted]

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Home > App registrations > Tenable Identity Collector

Tenable Identity Collector | API permissions

Search Refresh Got feedback?

Overview
Quickstart
Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

ℹ Successfully granted admin consent for the requested permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for [redacted]

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				
AuditLog.Read.All	Application	Read all audit log data	Yes	✅ Granted for [redacted]
Directory.Read.All	Application	Read directory data	Yes	✅ Granted for [redacted]
IdentityProvider.Read.All	Application	Read identity providers	Yes	✅ Granted for [redacted]
Policy.Read.All	Application	Read your organization's policies	Yes	✅ Granted for [redacted]
Reports.Read.All	Application	Read all usage reports	Yes	✅ Granted for [redacted]
RoleManagement.Read.All	Application	Read role management data for all RBAC providers	Yes	✅ Granted for [redacted]
UserAuthenticationMethod.Reac	Application	Read all users' authentication methods	Yes	✅ Granted for [redacted]

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

4. Después de configurar todas las opciones obligatorias en Microsoft Entra ID:

- [En Tenable Vulnerability Management, cree una nueva credencial de tipo "Microsoft Azure".](#)




- b. Seleccione el método de autenticación "Clave" e ingrese los valores que recuperó en el procedimiento anterior: ID de inquilino, ID de aplicación y Secreto de cliente.

Activar la compatibilidad con Microsoft Entra ID

Para activar la compatibilidad con Microsoft Entra ID:

Nota: Para activar esta funcionalidad correctamente, el usuario de Tenable Cloud que creó la clave de acceso y las claves secretas deben tener privilegios administrativos en el contenedor de Tenable Cloud al que hace referencia la licencia de Tenable Identity Exposure. Para obtener más información, consulte [Otorgamiento de licencias de Tenable Identity Exposure](#).

1. En Tenable Identity Exposure, haga clic en el ícono "Sistema"  en el menú de navegación izquierdo.
2. Haga clic en la pestaña **Configuración**.
Se abre la página **Configuración**.
3. En "Servicios de aplicación", haga clic en **Tenable Cloud**.
4. En **Activar compatibilidad con Microsoft Entra ID**, haga clic en el conmutador para habilitarla.
5. Si aún no inició sesión en [Tenable Cloud](#), haga clic en el vínculo para ir a la página de inicio de sesión:
 - a. Haga clic en **¿Olvidó la contraseña?** para solicitar un restablecimiento de la contraseña.
 - b. Escriba la dirección de correo electrónico asociada a su licencia de Tenable Identity Exposure y haga clic en **Solicitar restablecimiento de la contraseña**.

Tenable envía un correo electrónico a esa dirección con un vínculo para restablecer la contraseña.

Nota: Si la dirección de correo electrónico no es la misma que la asociada a la licencia de Tenable Identity Exposure, comuníquese con su servicio de atención al cliente para obtener asistencia.

6. Inicie sesión en Tenable Vulnerability Management.



7. Para [generar claves de API en Tenable Vulnerability Management](#), vaya a Tenable Vulnerability Management > **Configuración** > **Mi cuenta** > **Claves de API**.
8. Ingrese su AccessKey y SecretKey de usuario "Admin" de Tenable Vulnerability Management para establecer una conexión entre Tenable Identity Exposure y el servicio de Tenable Cloud.
9. Haga clic en **Editar claves** para enviar las claves de API.



Tenable Identity Exposure muestra un mensaje para confirmar que actualizó las claves de API.

Habilitar escaneos de inquilinos

Para agregar un nuevo inquilino de Microsoft Entra ID:

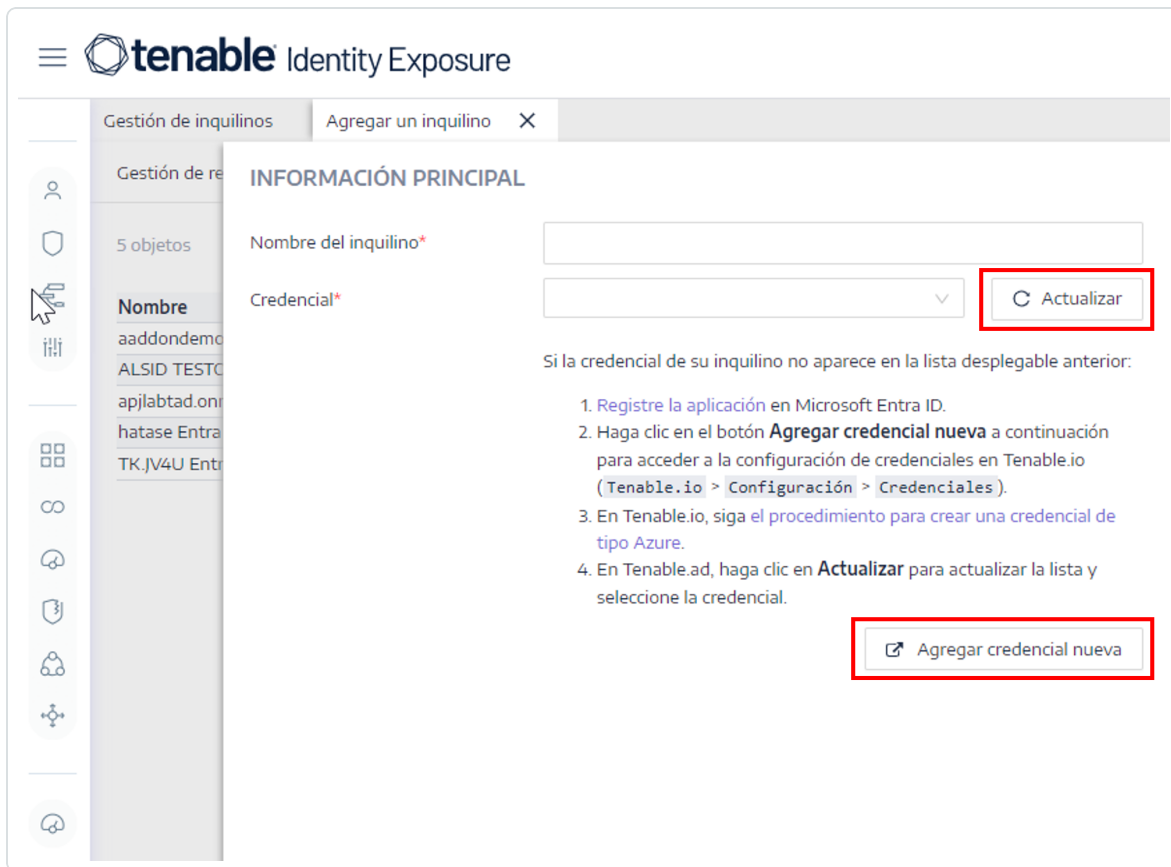
Al agregar un inquilino, se vincula Tenable Identity Exposure con el inquilino de Microsoft Entra ID para realizar escaneos en ese inquilino.

1. En la página "Configuración", haga clic en la pestaña **Gestión de inquilinos**.

Se abre la página **Gestión de inquilinos**.

2. Haga clic en **Agregar un inquilino**.

Se abre la página **Agregar un inquilino**.



3. En el cuadro **Nombre del inquilino**, escriba un nombre.
4. En el cuadro **Credenciales**, haga clic en la lista desplegable para seleccionar una credencial.
5. Si la credencial no aparece en la lista, puede:
 - Crear una en Tenable Vulnerability Management (Tenable Vulnerability Management > **Configuración** > **Credenciales**). Para obtener más información, consulte el [procedimiento para crear una credencial de tipo Azure](#) en Tenable Vulnerability Management.
 - Comprobar que tiene el [permiso "Puede usar" o "Puede editar" para la credencial](#) en Tenable Vulnerability Management. A menos que tenga estos permisos, Tenable Identity Exposure no muestra la credencial en la lista desplegable.
6. Haga clic en **Actualizar** para actualizar la lista desplegable de las credenciales.
7. Seleccione la credencial que creó.
8. Haga clic en **Agregar**.



Un mensaje confirma que Tenable Identity Exposure agregó el inquilino, que ahora aparece en la lista de la página “Gestión de inquilinos”.

Para habilitar escaneos para el inquilino:

Nota: Los escaneos de inquilinos no se producen en tiempo real y necesitan al menos 45 minutos para que los datos de Microsoft Entra ID se puedan ver en el Explorador de identidades.

- Seleccione un inquilino de la lista y haga clic en el conmutador para **Escaneo habilitado**.

Nombre	Proveedor	Estado del escaneo	Último escaneo correcto	Habilitar escaneo
aaddondemo5.onmicrosoft.com	Microsoft Entra ID	●	Miércoles, 23 de octubre de 2024 16:31	<input type="checkbox"/>
ALSID.TESTORG	Microsoft Entra ID	●	Miércoles, 23 de octubre de 2024 16:35	<input type="checkbox"/>

Tenable Identity Exposure solicita un escaneo del inquilino, y los resultados aparecen en la página “Indicador de exposición”.

Nota: El tiempo mínimo obligatorio de retraso entre dos escaneos es de **30 minutos**.

Recopilación de datos de Tenable Cloud

Tenable Cloud, la funcionalidad de recopilación de datos de Tenable Identity Exposure, transfiere su información a una nube privada para brindar análisis y servicios de seguridad. Para obtener más información sobre la recopilación de datos, consulte la declaración de [confianza y seguridad](#) de Tenable.

Para usar Tenable Cloud:

1. En Tenable Identity Exposure, haga clic en **Sistema** en la barra de navegación lateral y haga clic en **Sistema**.

Se abre el panel **Configuración del sistema**.

2. Seleccione la pestaña **Configuración**.

3. En la sección **Servicios de aplicación**, haga clic en **Tenable Cloud**.

Se abre el panel **Tenable Cloud**.



- Haga clic en el conmutador "Usar servicio de Tenable Cloud" para establecerlo en **Habilitado**.

Un mensaje confirma que Tenable Identity Exposure actualizó la configuración de la transferencia de información.

Usar el servicio de Tenable Cloud

Cuando se activa el servicio de Tenable Cloud, Tenable Identity Exposure transfiere la información que recopila a la nube privada de Tenable para brindarle más análisis de seguridad innovadores y nuevos servicios avanzados, en especial cuando usa otros productos de Tenable, entre otros.

Dado que la seguridad y la transparencia son fundamentales para nuestros valores corporativos, consulte nuestra declaración de [Confianza y seguridad](#) para obtener más información sobre cómo gestionamos los datos que recopilamos de usted.

 Al activar esta opción, indica que Tenable Identity Exposure también puede transferir a la nube privada de Tenable los datos que recopila a través del "análisis con privilegios" (cuando se configuró en sus dominios). Si no activa este servicio, Tenable no puede llevar a cabo ciertos análisis.

En funcionamiento

Análisis con privilegios

Análisis con privilegios es una funcionalidad opcional de Tenable Identity Exposure que requiere más privilegios (a diferencia de sus otras funcionalidades) para obtener datos que de otro modo estarían protegidos y brindar más análisis de seguridad.

Requisitos previos

Para utilizar Análisis con privilegios, tiene que abrir los puertos RPC dinámicos **TCP/49152-65535** y **UDP/49152-65535**. Para obtener información adicional, consulte [Matriz de flujos de red](#).

Obtención de datos

Nota: La funcionalidad Análisis con privilegios requiere privilegios elevados. Consulte [Acceso a Análisis con privilegios](#).



Cuando la funcionalidad Análisis con privilegios está habilitada, obtiene los siguientes datos adicionales:

- **Hashes de contraseñas:** Tenable Identity Exposure obtiene los hashes de LM y NT para el análisis de contraseñas. Tenable Identity Exposure obtiene los hashes de LM solo para advertir sobre su presencia, ya que usan un algoritmo antiguo y débil, pero no los almacena. El ámbito de la recopilación de hashes incluye:
 - Todas las cuentas de usuario habilitadas
 - Todas las cuentas de equipo de controladores de dominio habilitadas

Protección de datos

La instancia misma de Active Directory (AD) no almacena directamente las contraseñas de los usuarios, sino solo sus hashes mediante los algoritmos de hashes de LM o NT que no permiten recuperar la contraseña original. Tenable Identity Exposure no almacena hashes de LM.

A excepción de los clientes que hospedan sus instancias de Relay en una plataforma de SaaS-VPN, los hashes de contraseñas nunca salen de la infraestructura del cliente, ya que solo Relay los maneja. Relay no almacena contraseñas ni hashes de contraseñas, sino que recupera el hash de la contraseña del usuario cada vez que es necesario para el análisis y lo mantiene en su caché solo de manera temporal, en general solo unos pocos milisegundos.

Sin embargo, Tenable Identity Exposure conserva una cantidad mínima de bits de datos de hashes de contraseñas, almacenados de forma segura en la RAM de Relay, únicamente para llevar a cabo un análisis de [k-anonimato](#) para buscar usuarios con contraseñas idénticas.

Nota: Para los clientes de la plataforma de SaaS-VPN, el comportamiento es el mismo, pero es Tenable el que hospeda su instancia de Relay.

Registros de actividad

Los registros de actividad en Tenable Identity Exposure le permiten ver los rastros de todas las actividades que tuvieron lugar en la plataforma de Tenable Identity Exposure relacionadas con direcciones IP, usuarios o acciones específicos.

Para configurar los registros de actividad:



1. En **Gestión**, en el panel de navegación lateral de Tenable Identity Exposure, haga clic en **Sistema**.

Se abre el panel **Configuración del sistema**.

2. En la sección **Servicios de aplicación**, haga clic en **Registros de actividad**.

Se abre el panel **Gestión de registros de actividad**.

3. Para activar la funcionalidad de registros de actividad, haga clic en el conmutador para establecerlo en **Habilitado**.

4. En el cuadro "Duración de la retención (en meses)", haga clic en ► para seleccionar la cantidad de meses durante los cuales registrar actividades.

5. Haga clic en **Guardar**.

Un mensaje confirma que Tenable Identity Exposure actualizó la configuración.

The screenshot shows the Tenable Identity Exposure configuration page. The top navigation bar includes the Tenable logo and the text 'Identity Exposure'. On the right side of the navigation bar, there are several icons: a heart, a question mark, a notification bell with '99%', a gear, a grid, and a 'QA' button. Below the navigation bar, there are tabs for 'Configuración del sistema', 'Gestión de retransmisiones', 'Gestión de bosques', 'Gestión de dominios', 'Gestión de inquilinos', 'Configuración', 'Acerca de', and 'Información legal'. The 'Configuración' tab is selected. The main content area is divided into two columns. The left column is titled 'SERVICIOS DE APLICACIÓN' and contains a list of services: 'Servidor SMTP', 'Registros de actividad' (highlighted), 'Entidades de certificación de confianza', 'Indicadores de ataque', 'Tenable Cloud', 'Retransmisión', and 'Verificación de estado'. Below this is the 'MOTOR DE ALERTAS' section with 'SYSLOG' and 'Correo electrónico'. The 'INFORMES' section has 'Centro de informes'. The 'AUTENTICACIÓN' section has 'Tenable.one'. The right column is titled 'GESTIÓN DE REGISTROS DE ACTIVIDAD' and contains a toggle switch for 'Activar la característica Registros de actividad' which is turned on. Below it is a dropdown menu for 'Duración de la retención (en meses)*' with the value '6' selected. At the bottom right of the page, there is a red-bordered box with the text 'Borrar todos los datos de los registros de actividad' and a 'Guardar' button.

Para borrar los datos de los registros de actividad:



1. En **Gestión**, en el panel de navegación lateral de Tenable Identity Exposure, haga clic en **Sistema**.

Se abre el panel **Configuración del sistema**.

2. En la sección **Servicios de aplicación**, haga clic en **Registros de actividad**.

Se abre el panel **Gestión de registros de actividad**.

3. En **Borrar todos los datos de los registros de actividad**, haga clic en **Borrar**.

Aparece un mensaje para pedirle que confirme la acción.

4. Haga clic en **Confirmar**.


Un mensaje confirma que Tenable Identity Exposure actualizó la configuración.

Para establecer permisos para los registros de actividad propios de un usuario:

1. En **Gestión**, en el panel de navegación lateral de Tenable Identity Exposure, haga clic en **Cuentas**.

Aparece el panel **Gestión de cuentas de usuario**.

2. Seleccione la pestaña **Gestión de roles**.

3. En la lista de roles, pase el cursor por el rol de usuario que requiere este permiso y haga clic en el ícono  al final de la línea.

Se abre el panel **Editar un rol**.

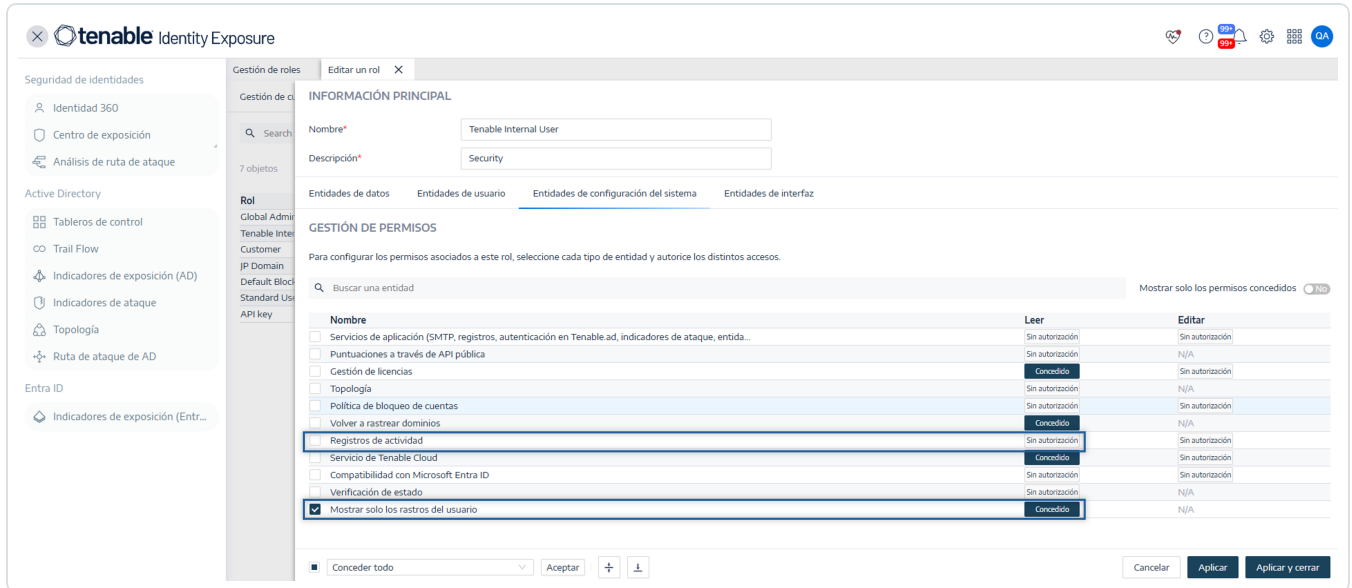
4. En la sección **Información principal**, seleccione la pestaña **Entidades de configuración del sistema**.

5. En la sección **Gestión de permisos**, haga lo siguiente:

- Anule la selección del permiso para **Registros de actividad** para establecerlo en *Sin autorización*.
- Seleccione el permiso para **Mostrar solo los rastros del usuario** en *Concedido*.

6. Haga clic en **Aplicar y cerrar**.

Un mensaje confirma que Tenable Identity Exposure actualizó el rol de usuario.



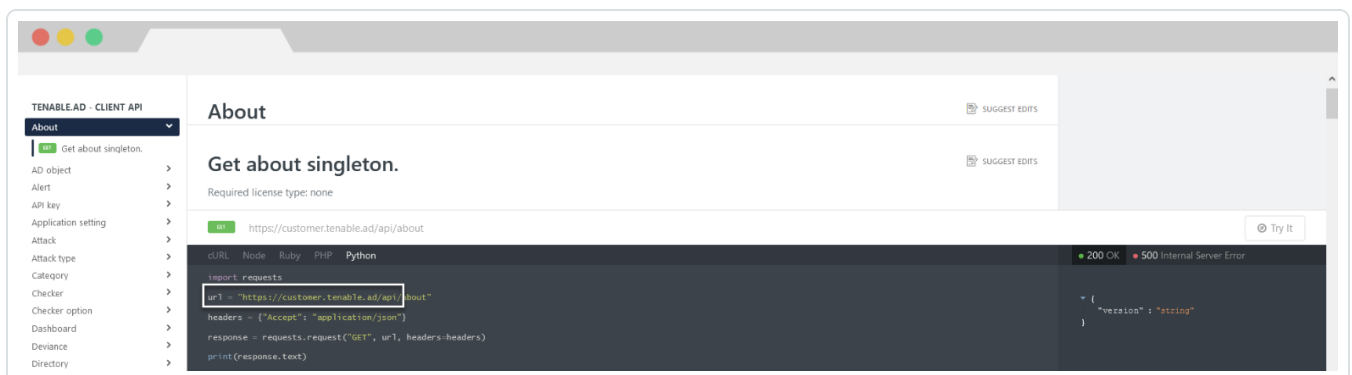
API pública de Tenable Identity Exposure

La API de Tenable Identity Exposure le permite comunicarse con sus servicios de bases de datos.

El archivo de OpenAPI que contiene la estructura y los recursos de la API de Tenable Identity Exposure está disponible [aquí](#).

Para acceder a la API para su instancia de Tenable Identity Exposure:

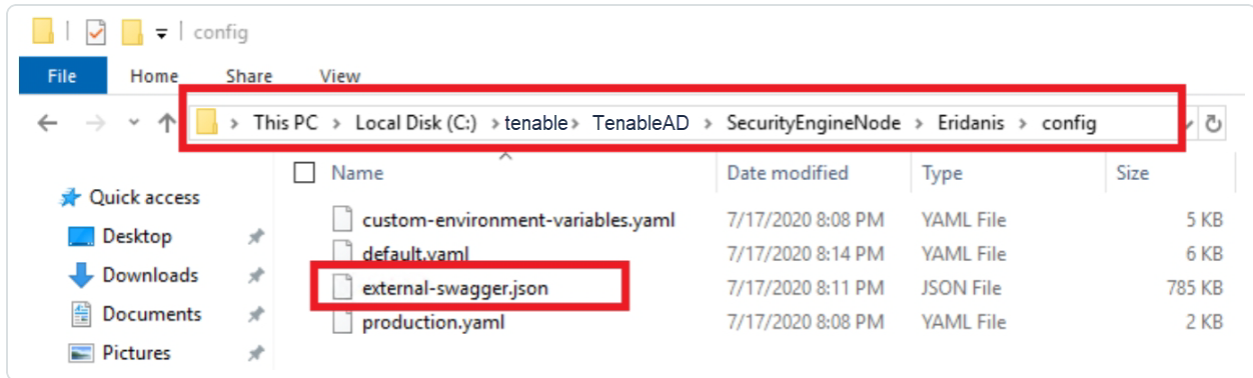
- En el navegador, abra esta [URL](#):





Para descargar el archivo de OpenAPI:

- Para instalaciones locales, siga esta ruta hasta Security Engine Node:



- Para instalaciones de SaaS, vaya al [Explorador de API de Tenable Identity Exposure](#).

Para recuperar una clave de API:

1. En Tenable Identity Exposure, haga clic en el ícono de su perfil de usuario y seleccione **Preferencias**.

Se abre el panel "Preferencias".

2. Desde el menú, seleccione **Clave de API**.

Tenable Identity Exposure muestra la clave de API actual.

3. Para copiar la clave de API en el portapapeles, haga clic en .

Para actualizar una clave de API:

Los tokens de acceso vencen si hace clic en **Actualizar clave de API** o si pierde el derecho a generar una clave de API o un token de acceso. El vencimiento no se relaciona con el tiempo ni con la cantidad de solicitudes de API. La generación o actualización de una clave de API es específica del usuario actual y no interfiere con otras claves de API de la cuenta. Cuando se obtiene una clave de API, también se recibe un token de actualización. Puede usar este token de actualización para recuperar una nueva clave de API.

Precaución: Cuando se actualiza la clave de API, Tenable Identity Exposure desactiva la clave de API actual. También recibirá un token de actualización.



1. Haga clic en **Actualizar clave de API**.

Aparece un mensaje para pedirle la confirmación.

2. Haga clic en **Confirmar**.

Gestión de datos

Tenable Identity Exposure conserva datos de Microsoft Entra ID y Active Directory durante un plazo máximo de 15 meses.

Capacidad	Período de retención
Ruta de ataque	6 meses
Topología	
Trail Flow	
Tableros de control e informes	12 meses
Centro de exposición	Hasta 15 meses
Identidad 360	
Indicadores de exposición (Entra ID)	
Indicadores de exposición (Active Directory)	<ul style="list-style-type: none">• Problemas activos: se conservan de manera indefinida
Indicadores de ataque (Active Directory)	<ul style="list-style-type: none">• Problemas resueltos: se conservan durante 6 meses

Para obtener más información, consulte [Datos de la plataforma Tenable Cloud](#).

Regiones de implementación

Actualmente, Tenable Identity Exposure SaaS se implementa en las siguientes regiones de Azure:

País	Región de Azure
América	



Brasil (São Paulo)	Sur de Brasil
Canadá (Ciudad de Quebec)	Este de Canadá
Canadá (Toronto)	Centro de Canadá
Estados Unidos (California)	Oeste de EE. UU.
Estados Unidos (Iowa)	Centro de EE. UU.
Estados Unidos (Virginia)	Este de EE. UU. 2
Europa, Oriente Medio, África	
Francia (París)	Centro de Francia
Irlanda	Norte de Europa
Países Bajos	Oeste de Europa
Sudáfrica (Johannesburgo)	Norte de Sudáfrica
Suiza (Zúrich)	Norte de Suiza
Emiratos Árabes Unidos (Dubái)	Norte de EAU
Reino Unido (Londres)	Sur del Reino Unido
Asia-Pacífico	
Australia (Nueva Gales del Sur)	Este de Australia
Australia (Victoria)	Sudeste de Australia
Hong Kong	Este de Asia
India (Pune)	Centro de la India
Japón (Osaka)	Oeste de Japón
Singapur	Sudeste de Asia

Otorgamiento de licencias de Tenable Identity Exposure




En este tema se desglosa el proceso de otorgamiento de licencias para Tenable Identity Exposure como producto independiente. También se explica cómo se contabilizan los activos y se describe qué sucede durante los períodos de excedencia o vencimiento de las licencias.

Licencias de Tenable Identity Exposure

Tenable Identity Exposure tiene dos versiones: una versión en la nube y una versión local. En algunos casos, Tenable también ofrece precios de suscripción.

Para usar Tenable Identity Exposure, tiene que comprar licencias según las necesidades de la organización y los detalles del entorno. Tenable Identity Exposure luego asigna esas licencias a sus *activos*: usuarios habilitados en sus servicios de directorio.

Cuando el entorno se expande, lo mismo sucede con la cantidad de activos, por lo que compra más licencias para tener en cuenta el cambio. Las licencias de Tenable usan precios progresivos, por lo que, cuanto más compre, menor será el precio por unidad. Para conocer los precios, comuníquese con su representante de Tenable.

Sugerencia: Para ver el recuento actual de licencias y activos disponibles, en la barra de navegación superior de Tenable, haga clic en  y luego en **Información sobre licencias**. Para obtener más información, consulte la página [License Information](#) (Información de licencias).

Nota: Tenable ofrece precios simplificados para los proveedores de servicios de seguridad administrados (MSSP). Para obtener más información, comuníquese con su representante de Tenable.

Cómo se contabilizan los activos

Cada licencia de Tenable Identity Exposure que compra le da derecho a escanear una identidad única o representación digital de un usuario. Tenable no cuenta dos veces las identidades. Por ejemplo, las cuentas de usuario habilitadas para la misma identidad tanto en Microsoft Active Directory como en Microsoft Entra ID cuentan como una licencia de Tenable.

Use este script de PowerShell para rastrear cuentas de usuario habilitadas en AD:

```
(Get-ADuser -Filter 'enabled -eq $true').count
```

Use este script de PowerShell para rastrear cuentas de usuario habilitadas en Entra ID:



```
(Get-MgUser -All -Filter "accountEnabled eq true" -Property onPremisesSyncEnabled | where {  
$_onPremisesSyncEnabled -ne $true }).Count
```

Componentes de Tenable Identity Exposure

Ambas versiones de Tenable Identity Exposure incluyen los siguientes componentes:

- Trail Flow
- Topología
- Indicadores de exposición
- Indicadores de ataque
- Rutas de ataque
- Centro de exposición
- Compatibilidad con Microsoft Entra ID

Recuperación de licencias

Cuando compra licencias, el recuento total de licencias permanece estático durante la vigencia del contrato, a menos que compre más licencias. Sin embargo, Tenable Identity Exposure recupera licencias en tiempo real cuando elimina usuarios habilitados del servicio de directorios de su entorno.

Superar el límite de licencias

Para permitir picos de uso debido a actualizaciones de hardware, crecimiento repentino del entorno o amenazas imprevistas, las licencias de Tenable son elásticas. Puede exceder temporalmente el recuento de identidades autorizadas en un 10 %. No obstante, cuando escanea más identidades de para las que tiene licencia, Tenable comunica claramente el exceso y luego reduce la funcionalidad en tres etapas.

Nota: Para entornos locales que utilizan Tenable Identity Exposure 3.77 o una versión posterior, la aplicación de licencias es inmediata.



Situación	Resultado
Tiene más identidades habilitadas que las que tienen licencia durante tres días consecutivos.	Aparece un mensaje en Tenable Identity Exposure.
Tiene más identidades habilitadas que las que tienen licencia durante más de 15 días.	Aparece un mensaje y una advertencia sobre la funcionalidad reducida en Tenable Identity Exposure.
Tiene más identidades habilitadas que las que tienen licencia durante más de 45 días.	Aparece un mensaje en Tenable Identity Exposure y no puede usar la funcionalidad Indicador de exposición en la interfaz de usuario ni en la API.

Licencias vencidas

Las licencias de Tenable Identity Exposure que compra son válidas durante la vigencia del contrato. Treinta (30) días antes de que expire la licencia, aparecerá una advertencia en la interfaz de usuario. Durante este período de renovación, comuníquese con su representante de Tenable para agregar o quitar productos o para cambiar la cantidad de licencias.

Una vez que la licencia venza, ya no podrá iniciar sesión en la plataforma de Tenable.

Gestionar la licencia

Tenable Identity Exposure requiere un archivo de licencia de Tenable o gestionado a través de socios empresariales autorizados. El recuento de usuarios con licencia cubre todas las cuentas de usuario y de servicio habilitadas.

Debe cargar el archivo de licencia para configurar y usar Tenable Identity Exposure.

Sugerencia: El archivo de licencia se encuentra en el portal de Tenable Community, en "My Products" (Mis productos) (tiene que ser administrador de Tenable Community para ver el archivo de licencia).

Precaución: Si no aplica una licencia válida a la plataforma de SaaS, Tenable la dará de baja después de un período determinado.

Las licencias de Tenable Identity Exposure pueden incluir:




- Indicadores de ataque
- Indicadores de exposición
- Ambos

Para ver la licencia:

- En Tenable Identity Exposure, haga clic en la pestaña **Sistema**  > **Acerca de**.

Aparece la licencia.



The screenshot shows the 'About' page in Tenable Identity Exposure. The 'About' tab is selected in the top navigation bar. The page displays the following information:

LICENCIA	
Nombre del cliente	Tenable - Sales APAC
Tipo de licencia	Licencia para uso interno únicamente
Características	- Indicadores de ataque - Indicadores de exposición
Usuarios activos actuales	2 968
Usuarios activos concedidos por la licencia	10 000
Fecha de vencimiento	1 de enero de 2025
Asociación de productos	Tenable One
Código de activación	1111-1111-1111-1111-1111
ID de contenedor de Tenable Cloud	2084471-8483-4428-8337-49F03B4F4716

Consumo de la licencia

Para instalaciones locales, Tenable Identity Exposure hace un seguimiento del consumo de la licencia si hay disponible una conexión a internet.

Prevención de errores de coincidencia de UUID de contenedores

En Tenable Identity Exposure, cada licencia incluye un UUID de contenedor exclusivo, que vincula la aplicación a un contenedor de Tenable Cloud específico. Este UUID de contenedor debe permanecer constante para garantizar una integración perfecta y evitar problemas operativos.



Para evitar incoherencias en el UUID de contenedor (por ejemplo, cuando se carga una nueva licencia después de una renovación), Tenable Identity Exposure puede detectar “errores de coincidencia” de UUID de contenedores.

Si intenta cargar una licencia con otro UUID de contenedor, aparecerá el mensaje “No se puede cambiar el contenedor de Tenable Cloud”. Es posible que se encuentre en una de las siguientes situaciones:

- Migración de la licencia independiente de Tenable Identity Exposure a una licencia de Tenable One.
- Migración del contenedor de un sitio de AWS de Tenable a otro.
- Vencimiento del contenedor anterior y creación de uno nuevo.

Si se encuentra en uno de estos casos, comuníquese con Tenable para analizar la posibilidad de cambiar el contenedor de Tenable Cloud para esta plataforma de Tenable Identity Exposure.

Validez de la licencia

La licencia de Tenable Identity Exposure seguirá siendo válida siempre que cumpla con los siguientes criterios:

- La cantidad de usuarios activos no supera el número concedido en la licencia. Tenable Identity Exposure muestra tres tipos de mensajes de advertencia según el caso.
 - La cantidad de usuarios activos **está próxima al límite** establecido en las condiciones de la licencia: tiene que actualizar la licencia.
 - La cantidad de usuarios activos **supera** las condiciones de la licencia: tiene que actualizar la licencia.
 - La cantidad de usuarios activos **supera las condiciones de la licencia (en un 10 %)**: ya no tiene acceso a la página “Indicador de exposición” y tiene que actualizar la licencia.
- La fecha de vencimiento no pasó.

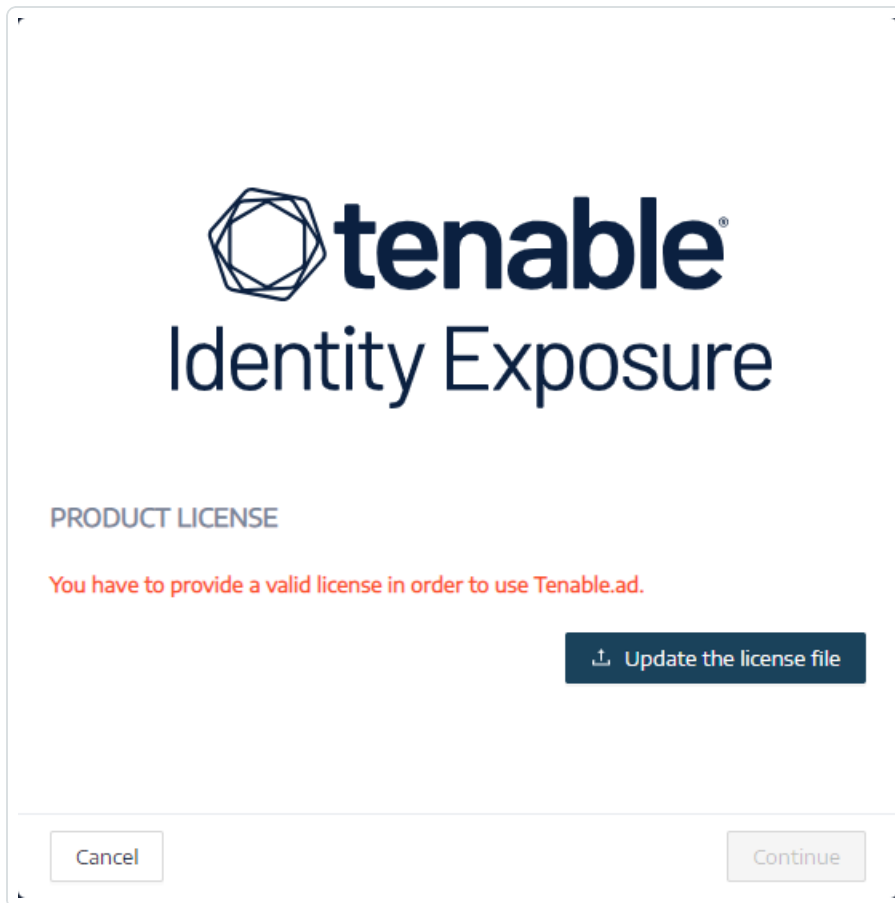
Si no cumple con alguno de los criterios anteriores, Tenable Identity Exposure muestra una advertencia para solicitarle que actualice la licencia:

THE LICENSE HAS EXPIRED.
Please update the license file or contact Tenable support.



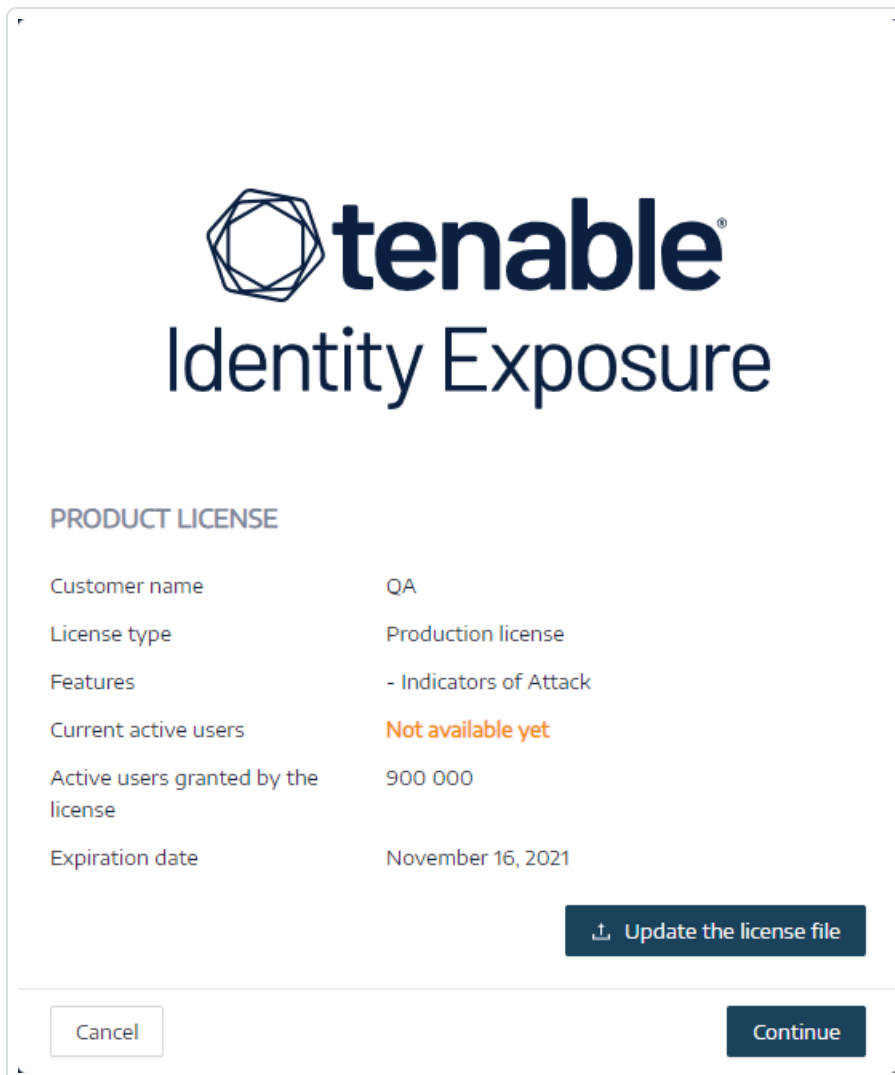
Para cargar un archivo de licencia:

1. Desde la ventana de inicio de sesión, haga clic en **Actualizar el archivo de licencia**.



2. Busque la ubicación del archivo de licencia y haga clic en **Abrir**.

En el siguiente ejemplo se muestra un archivo de licencia aplicado correctamente:



3. Haga clic en **Continuar** para abrir Tenable Identity Exposure.

Para actualizar un archivo de licencia:

1. En Tenable Identity Exposure, haga clic en **Sistema** y **Acerca de**.
2. Haga clic en **Actualizar el archivo de licencia**.
3. Busque la ubicación del archivo de licencia y haga clic en **Abrir**.

Tenable Identity Exposure actualiza el archivo de licencia. En el caso de un archivo de licencia no válido, comuníquese con el servicio de atención al cliente.

Soporte a largo plazo (LTS) frente a versiones normales: diferencias y ventajas clave



¿Qué es LTS?

Las versiones LTS (soporte a largo plazo) son versiones de software que mantenemos durante un período prolongado: 18 meses. Durante este plazo, ofrecemos actualizaciones periódicas, como parches de seguridad y correcciones de errores críticos, sin introducir nuevas características que puedan interrumpir la funcionalidad existente.

Las versiones LTS están diseñadas para clientes que priorizan la estabilidad, la confiabilidad y el mantenimiento a largo plazo frente a las características más recientes. Estas versiones son ideales para entornos donde las actualizaciones o cambios frecuentes podrían generar tiempos de inactividad o costos adicionales para realizar pruebas e implementaciones.

¿Qué son las versiones normales?

Las versiones normales son nuestras publicaciones de software estándar, que incluyen nuevas características, mejoras y actualizaciones. Estas versiones son más dinámicas y se actualizan con frecuencia (cada 6 meses), pero reciben soporte durante un período más corto en comparación con las versiones LTS.

Las versiones normales son ideales para los clientes que quieren mantenerse a la vanguardia de la tecnología y adoptar periódicamente nuevas características y actualizaciones, incluso si esto requiere actualizaciones más frecuentes.

Diferencias clave entre las versiones LTS y normales:

- **Duración del soporte:** las versiones LTS reciben soporte durante 18 meses, mientras que las versiones normales reciben soporte durante 6 meses.
- **Estabilidad frente a innovación:** LTS se centra en la estabilidad y la seguridad, y tiene cambios mínimos en las características; mientras que las versiones normales ponen el énfasis en la innovación e introducen nuevas características con mayor frecuencia.
- **Frecuencia de actualización:** los clientes que usan versiones LTS actualizan con menos frecuencia, mientras que aquellos que usan versiones normales pueden necesitar actualizar con mayor frecuencia para mantenerse al día.

¿Por qué elegir LTS?



Las versiones LTS son perfectas para sistemas de misión crítica o entornos donde el tiempo de inactividad es costoso. Ofrecen tranquilidad, ya que garantizan que la versión se mantenga estable y con soporte a largo plazo.

¿Por qué elegir las versiones normales?

Si valora tener las características y mejoras más recientes, las versiones normales son más adecuadas. Si bien pueden exigir actualizaciones más frecuentes, brindan acceso a las funcionalidades más nuevas.

Solucionar problemas de Tenable Identity Exposure

Los siguientes temas lo ayudarán con los problemas que puedan surgir al usar Tenable Identity Exposure (anteriormente conocido como Tenable.ad):

- [Herramienta de diagnóstico de Tenable Identity Exposure](#)
- [Interferencia de endurecimiento de SYSVOL con Tenable Identity Exposure](#)

Registros para solucionar problemas

Tenable Identity Exposure ofrece registros de depuración para solucionar problemas y comprender el comportamiento de la plataforma.

Los siguientes son algunos de los registros más comunes:

- Registros de instalación o actualización
- Registros de la plataforma
- Registros de instalación o actualización de scripts de loA

Registros de instalación o actualización

Si el programa de instalación no puede instalar Tenable Identity Exposure en una máquina, se puede reenviar el archivo de registros a nuestra comunidad de soporte (<https://community.tenable.com/s/>).

Este archivo de registros se encuentra en la carpeta %tmp% y su nombre siempre comienza por "MSI" seguido de números aleatorios, como MSI65931.LOG.



Para generar archivos de registros en otra ubicación (por ejemplo, si colocó el instalador en el escritorio):

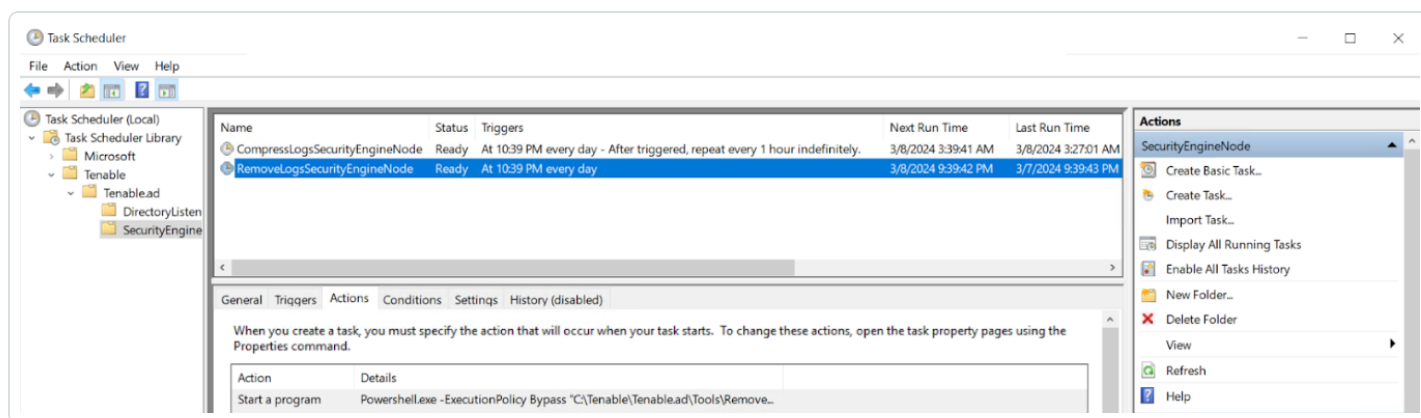
1. En la línea de comandos de la máquina local, escriba `cd desktop`.
2. Escriba `.\installname.exe /LOGS "c:\<ruta>\logsmis1.txt"`.

Registros de la plataforma

Tenable Identity Exposure genera archivos de registros para los distintos servicios en la instalación individual.

- Desde el servidor de Directory Listener: <carpeta de instalación>\DirectoryListener\logs
- Desde el servidor de Security Engine Node: <carpeta de instalación>\SecurityEngineNode\logs
- Desde el servidor de Storage Manager: <carpeta de instalación>\StorageManager\logs
- Desde el servidor de Directory Listener o el servidor de Secure Relay independiente: <carpeta de instalación>\SecureRelay\logs

Los archivos de registros predeterminados de la plataforma rotan cuando alcanzan un tamaño de 100 MB cada uno y luego se comprimen. Estas tareas se generan automáticamente durante la instalación en el Programador de tareas de Windows. El siguiente es un ejemplo de las tareas en el nodo de Security Engine Node.



Registros de instalación o actualización de scripts de loA



El script de indicadores de ataque (IoA) crea un archivo de registros (por ejemplo, `Register-TenableIOA-xxxx.log`) en la misma ubicación que el script. Puede revisarlo si hay algún error o problema durante la instalación.

Períodos de retención de registros

- **Retención a corto plazo:** conserve los registros de depuración durante un período corto, como 7 días después de su generación. Esto le permite diagnosticar problemas recientes y minimizar el consumo de almacenamiento.
- **Archivado a largo plazo:** considere archivar un subconjunto de registros de depuración durante períodos más prolongados con fines de cumplimiento o resolución de problemas. Puede almacenarlos en una ubicación segura o comprimirlos para usar el espacio de manera eficiente.

Herramienta de diagnóstico de Tenable Identity Exposure

Tenable Identity Exposure proporciona una herramienta de diagnóstico que le permite recuperar información sobre registros relacionada con su instalación de Tenable Identity Exposure para que el servicio de atención al cliente pueda analizarla y ayudarlo con cualquier problema.

Puede descargar esta herramienta de diagnóstico desde el portal de descargas de Tenable.

Nota: Esta herramienta de diagnóstico solo funciona para **instalaciones locales** de Tenable Identity Exposure.

La herramienta de diagnóstico puede hacer lo siguiente:

- Identificar si la máquina actual (donde inició el archivo ejecutable) hospeda el componente Storage Manager (SM), Security Engine Node (SEN) o Directory Listener (DL).
- Escanear el entorno para buscar otras instalaciones de Tenable Identity Exposure disponibles en su red.
- Detectar una lista de orígenes de registros relacionados con sus instalaciones de Tenable Identity Exposure para probarlos y recuperar información sobre ellos según corresponda.
- Recuperar registros de MSI en intentos fallidos de instalación de Tenable Identity Exposure.

Algunos consejos para obtener mejores resultados



- Ejecute la herramienta de diagnóstico en la instancia de SEN.
- Ejecute la herramienta de diagnóstico con un usuario elevado para activar la mayoría o todos los orígenes de registros.
- Para detectar la instancia de SM u otra instalación, verifique que se cumplan las siguientes condiciones:
 - La configuración permite que el comando remoto se ejecute en el equipo remoto (cmdlet Invoke-Command).
 - La configuración permite el acceso remoto a los discos.
 - WMI se habilitó y se permite en la cuenta de usuario actual.

Para ejecutar la herramienta de diagnóstico:

1. Descargue el archivo `TenableAdDiagnosticTool.OnPrem.Console.exe` del [portal de descargas de Tenable](#).
2. Ejecute el archivo ejecutable como administrador en una máquina con Tenable Identity Exposure, preferiblemente la que hospeda la instancia de SEN.
3. Cuando se le solicite, escriba una de las siguientes opciones:
 - `E`: todos los registros (opción predeterminada)
 - `Msi`: registros relacionados con instalaciones de Tenable Identity Exposure
 - `Tenable`: registros relacionados con Tenable Identity Exposure

4. Presione Intro.

La herramienta de diagnóstico escanea su instalación. Cuando se completa el escaneo, el resultado es un archivo comprimido que se encuentra en su directorio actual.

5. Envíe este archivo comprimido al servicio de atención al cliente de Tenable Identity Exposure. Asegúrese de no modificar el contenido del archivo de ninguna manera.

Para ejecutar la herramienta de diagnóstico mediante la línea de comandos:



1. En la línea de comandos, ejecute el archivo ejecutable `TenableAdDiagnosticTool.OnPrem.Console.exe` como administrador en la máquina con Tenable Identity Exposure, preferiblemente la que hospeda la instancia de SEN.

La herramienta de diagnóstico escanea su instalación. Cuando se completa el escaneo, el resultado es un archivo comprimido que se encuentra en su directorio actual.

2. Envíe este archivo comprimido al servicio de atención al cliente de Tenable Identity Exposure. Asegúrese de no modificar el contenido del archivo de ninguna manera.

Otras opciones

La herramienta de diagnóstico también ofrece las siguientes opciones mediante la línea de comandos:

- `-- help`: breve descripción del uso de la herramienta de diagnóstico.
- `-- commands`: lista de consultas de PowerShell o WMI para probar las capacidades de la máquina y escanear otras instalaciones.

Interferencia de endurecimiento de SYSVOL con Tenable Identity Exposure

SYSVOL es una carpeta compartida que se encuentra en cada controlador de dominio (DC) en un dominio de Active Directory. Allí se almacenan las carpetas y archivos para las políticas de grupo (GPO). El contenido de SYSVOL se replica en todos los controladores de dominio y se accede a él a través de rutas con convención de nomenclatura universal (UNC) como `\\<ejemplo.com>\SYSVOL` o `\\<IP_o_FQDN_de_DC>\SYSVOL`.

El **endurecimiento de SYSVOL** hace referencia al uso del parámetro Rutas endurecidas de UNC, también conocido como "acceso endurecido de UNC", "rutas de acceso UNC protegidas", "endurecimiento de rutas UNC", "rutas protegidas", etc. Esta funcionalidad surgió para responder a la vulnerabilidad MS15-011 (KB 3000483) en la política de grupo. Muchos estándares de ciberseguridad, como CIS Benchmarks, exigen la aplicación de esta funcionalidad.

Cuando se aplica este parámetro de endurecimiento en los clientes del Bloque de mensajes del servidor (SMB), en realidad aumenta la seguridad de las máquinas unidas a un dominio para garantizar que el contenido del GPO que recuperan de SYSVOL esté libre de manipulación por parte de un atacante en la red. No obstante, en ciertas situaciones, este parámetro también puede interferir con el funcionamiento de Tenable Identity Exposure.



Siga las instrucciones de esta sección de solución de problemas si observa que las rutas de acceso UNC protegidas perturban la conectividad entre Tenable Identity Exposure y el recurso compartido SYSVOL.

Entornos afectados

Las siguientes opciones de implementación de Tenable Identity Exposure pueden experimentar este problema:

- En el entorno local
- SaaS con Secure Relay

Esta opción de implementación no se ve afectada:

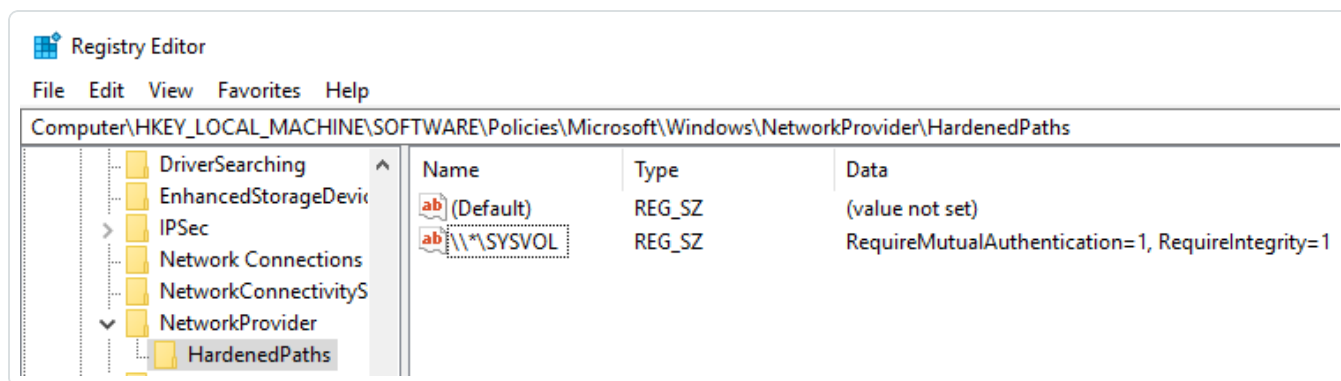
- SaaS con VPN

El endurecimiento de SYSVOL es un parámetro del lado del cliente, lo que significa que opera en las máquinas que se conectan al recurso compartido de SYSVOL y no en los controladores de dominio.

Windows habilita este parámetro de manera predeterminada y puede interferir con Tenable Identity Exposure.

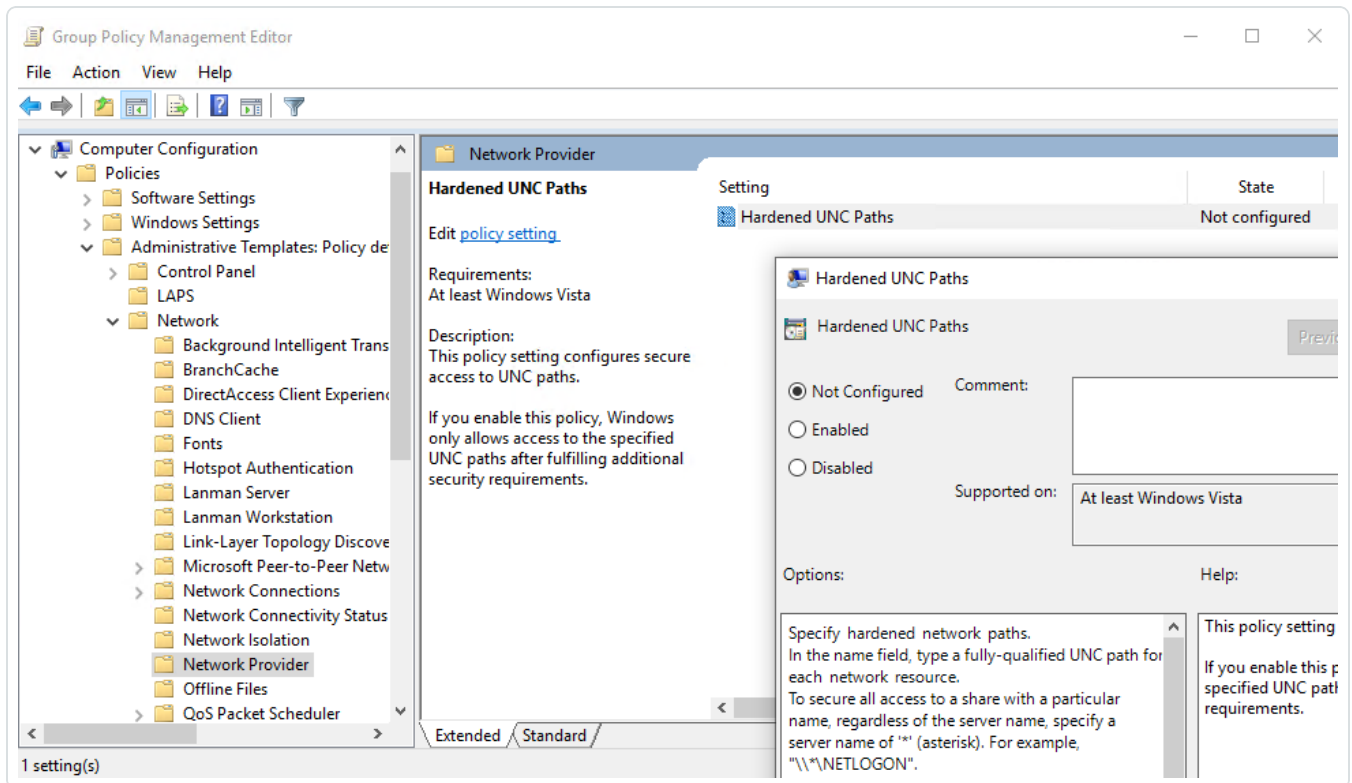
Algunas organizaciones también buscan garantizar la activación de este parámetro y aplicarlo mediante la configuración del GPO relacionado o al definir directamente la clave del registro correspondiente.

- Puede encontrar las claves del registro relacionadas con las rutas de acceso UNC protegidas en "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths":





- Puede encontrar la configuración del GPO correspondiente en “Configuración del equipo/Plantillas administrativas/Red/Proveedor de red/Rutas de acceso UNC protegidas”:



La aplicación de medidas de endurecimiento de SYSVOL se produce cuando una ruta de acceso UNC que hace referencia a SYSVOL (por ejemplo, "*\SYSVOL") tiene los parámetros "RequireMutualAuthentication" y "RequireIntegrity" establecidos en el valor "1".

Señales de problemas de endurecimiento de SYSVOL

Cuando sospeche que el endurecimiento de SYSVOL interfiere con Tenable Identity Exposure, compruebe lo siguiente:

1. En Tenable Identity Exposure, vaya a **Sistema > Gestión de dominios** para ver el estado de inicialización de LDAP y SYSVOL para cada dominio.

Un dominio con conectividad normal muestra un indicador verde, mientras que un dominio con problemas de conectividad puede mostrar un indicador de rastreo que continúa sin cesar.



Nombre	Bosque	Dirección IP o FQDN	Estado de inicialización de LDAP	Estado de inicialización de SYSVOL	Análisis con privilegios	Estado de configuración de la cuenta señuelo
ALSID	ALSID.CORP Forest (prod)	apjlab-dc.alsid.corp	●	●	●	●
Japan Domain @ Alsid.corp	ALSID.CORP Forest (prod)	apjlab-afad-dc-jp.alsid.corp	●	●	●	●
KHLAB	KHLAB forest	dc-vm.tenable.ad	●	●	●	●
TCORP Domain	TCORP Forest	dc01.tcorp.local	●	●	●	●
TKLAB	JV4U Forest	tk-dc01.tk.jv4u.com	○	○	●	○

- En la máquina de Directory Listener o Relay, abra la carpeta de registros: <carpeta de instalación>\DirectoryListener\logs.
- Abra el archivo de registros de Ceti y busque la cadena “SMB mapping creation failed” o “Access is denied”. Los registros de errores que contienen esta frase indican que es probable que exista un endurecimiento de UNC en la máquina de Directory Listener o Relay.

```
[2022-12-28 09:46:17:312 UTC INFORMATION] SMB mapping removed for remote path '\\bcforest.lab\sysvol' {SourceContext="WmiSmbConnectionManagerNative", DirectoryId=1, Dns="bcforest.lab", Host="bcforest.lab", Source=SYSVOL, Version="3.29.4"}
[2022-12-28 09:46:17:312 UTC INFORMATION] Creating SMB mapping for client 'Listener' and remote path '\\bcforest.lab\sysvol' with user 'tservice'... {SourceContext="WmiSmbConnectionManagerNative", DirectoryId=1, Dns="bcforest.lab", Host="bcforest.lab", Source=SYSVOL, Version="3.29.4"}
[2022-12-28 09:46:17:314 UTC ERROR] An error has occurred while establishing SMB mapping. {SourceContext="WmiSmbConnectionManagerNative", DirectoryId=2, Dns="bcforest.lab", Host="bcforest.lab", Source=SYSVOL, Version="3.29.4"}
System.InvalidOperationException: The SMB mapping creation failed: ERROR_ACCESS_DENIED: Access is denied.
    at Alsid.DotNetLibs.Smb.Management.WmiSmbConnectionManagerNative.CreateAsync(SmbClient client, CancellationToken cancellationToken) in D:\a\1\s\DotNetLibs\Alsid.DotNetLibs.Smb.Management\WmiSmbConnectionManagerNative.cs:line 95
    at Alsid.DotNetLibs.Smb.Management.WmiSmbConnectionManagerNative.<c__DisplayClass10_0.<<EnsureSmbMappingIsMountedAsync>>b__0.MoveNext() in D:\a\1\s\DotNetLibs\Alsid.DotNetLibs.Smb.Management\WmiSmbConnectionManagerNative.cs:line 152
    --- End of stack trace from previous location ---
    at Polly.AsyncPolicy.<c__DisplayClass40_0.<<ImplementationAsync>>b__0.MoveNext()
    --- End of stack trace from previous location ---
    at Polly.Retry.AsyncRetryEngine.ImplementationAsync[TResult](Func`3 action, Context context, CancellationToken cancellationToken, ExceptionPredicates shouldRetryExceptionPredicates, ResultPredicates`1 shouldRetryResultPredicates, Func`1 retryInSeconds)
[2022-12-28 09:46:17:314 UTC ERROR] An error has occurred: 'The SMB mapping creation failed: ERROR_ACCESS_DENIED: Access is denied.'
'. Retry in '5 seconds'... {SourceContext="WmiSmbConnectionManagerNative", DirectoryId=2, Dns="bcforest.lab", Host="bcforest.lab", Source=SYSVOL, Version="3.29.4"}
System.InvalidOperationException: The SMB mapping creation failed: ERROR_ACCESS_DENIED: Access is denied.
    at Alsid.DotNetLibs.Smb.Management.WmiSmbConnectionManagerNative.CreateAsync(SmbClient client, CancellationToken cancellationToken) in D:\a\1\s\DotNetLibs\Alsid.DotNetLibs.Smb.Management\WmiSmbConnectionManagerNative.cs:line 95
    at Alsid.DotNetLibs.Smb.Management.WmiSmbConnectionManagerNative.<c__DisplayClass10_0.<<EnsureSmbMappingIsMountedAsync>>b__0.MoveNext() in D:\a\1\s\DotNetLibs\Alsid.DotNetLibs.Smb.Management\WmiSmbConnectionManagerNative.cs:line 152
    --- End of stack trace from previous location ---
    at Polly.AsyncPolicy.<c__DisplayClass40_0.<<ImplementationAsync>>b__0.MoveNext()
    --- End of stack trace from previous location ---
    at Polly.Retry.AsyncRetryEngine.ImplementationAsync[TResult](Func`3 action, Context context, CancellationToken cancellationToken, ExceptionPredicates shouldRetryExceptionPredicates, ResultPredicates`1 shouldRetryResultPredicates, Func`1 retryInSeconds)
[2022-12-28 09:46:17:314 UTC ERROR] An error has occurred while establishing SMB mapping. {SourceContext="WmiSmbConnectionManagerNative", DirectoryId=1, Dns="bcforest.lab", Host="bcforest.lab", Source=SYSVOL, Version="3.29.4"}
System.InvalidOperationException: The SMB mapping creation failed: ERROR_ACCESS_DENIED: Access is denied.
```

Opciones de corrección

Hay dos posibles opciones de corrección: [Cambiar a la autenticación de Kerberos](#) o [Deshabilitar el endurecimiento de SYSVOL](#).

Cambiar a la autenticación de Kerberos

Esta es la opción preferida, ya que evita deshabilitar la funcionalidad de endurecimiento.

Únicamente cuando se conecta a los controladores de dominio supervisados mediante la autenticación de NTLM, el refuerzo de SYSVOL interfiere con Tenable Identity Exposure. Esto se debe a que NTLM no es compatible con el parámetro “RequireMutualAuthentication=1”. Tenable Identity Exposure también admite Kerberos. No es necesario deshabilitar el endurecimiento de SYSVOL si configura y usa Kerberos correctamente. Para obtener más información, consulte [Autenticación de Kerberos](#).



Deshabilitar el endurecimiento de SYSVOL

Si no puede cambiar a la autenticación de Kerberos, también tiene la opción de deshabilitar el endurecimiento de SYSVOL.

Windows habilita el endurecimiento de SYSVOL de manera predeterminada, por lo que no alcanza con eliminar la clave del registro o la configuración del GPO. Tiene que deshabilitarlo de manera explícita y aplicar este cambio solo en la máquina que hospeda el componente Directory Listener (local) o Relay (SaaS con Secure Relay). Esto no afecta a otras máquinas y no es necesario deshabilitar nunca el endurecimiento de SYSVOL en los controladores de dominio.

Los instaladores de Tenable Identity Exposure usados en la máquina que hospeda Directory Listener (local) o Relay (SaaS con Secure Relay) ya deshabilitan el endurecimiento de SYSVOL localmente. Sin embargo, es posible que un GPO o un script en su entorno elimine o sobrescriba la clave del registro.

Hay dos casos posibles:

- Si la máquina de Directory Listener o Relay **no está unida a un dominio**: no puede usar un GPO para configurar la máquina. Tiene que deshabilitar el endurecimiento de SYSVOL en el registro (consulte [Registro \(GUI\)](#) o [Registro \(PowerShell\)](#)).
- Si la máquina de Directory Listener o Relay **está unida a un dominio** (lo que Tenable Identity Exposure [no recomienda](#)): puede aplicar la configuración directamente en el registro (consulte [Registro \(GUI\)](#) o [Registro \(PowerShell\)](#)) o mediante un [GPO](#). Al seguir cualquiera de estos métodos, tiene que asegurarse de que un GPO o un script no sobrescriban la clave del registro. Tiene dos maneras de hacerlo:
 - Revisar atentamente todos los GPO que se aplican en esta máquina.
 - Aplicar el cambio y esperar un poco, o forzar la aplicación de los GPO con “gpupdate /force” y verificar que la clave del registro haya mantenido su valor.

Después de reiniciar la máquina de Directory Listener o Relay, el indicador de rastreo en el dominio modificado debería cambiar a un indicador verde:



Buscar un dominio

5 objetos

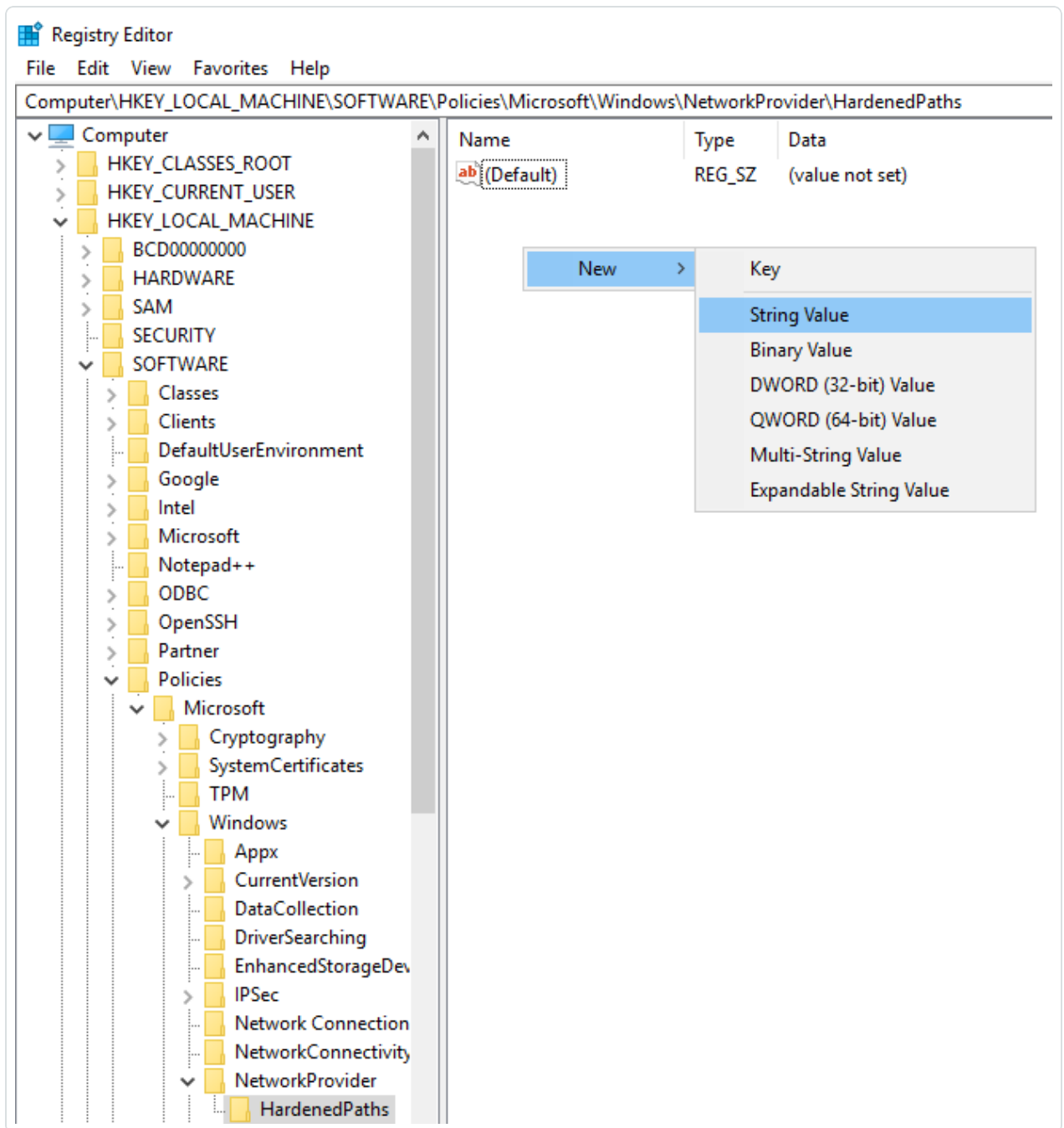
Nombre	Bosque	Dirección IP o FQDN	Estado de inicialización de LDAP	Estado de inicialización de SYSVOL	Análisis con privilegios	Estado de configuración de la cuenta señuelo
ALSID	ALSID.CORP Forest (prod)	apilab-dcalsid.corp	●	●	●	●
Japan Domain @ Alsid.corp	ALSID.CORP Forest (prod)	apilab-afad-dc-jp.alsid.corp	●	●	●	●
KHLAB	KHLAB forest	dc-vm.tenable.ad	●	●	●	●
TCORP Domain	TCORP Forest	dc01.tcorp.local	●	●	●	●
TK.JV4U	JV4U Forest	tk-dc1.tk.jv4u.com	●	●	●	●

Registro (GUI)

Para deshabilitar el endurecimiento de SYSVOL en el registro mediante la GUI:

1. Conéctese a la máquina de Directory Listener o Relay con derechos administrativos.
2. Abra el editor del registro y vaya a HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths.
3. Cree una clave llamada "*\SYSVOL" si no existe aún, de la siguiente manera:

- a. Haga clic con el botón derecho en el panel derecho y elija **Nuevo > Valor de cadena**.



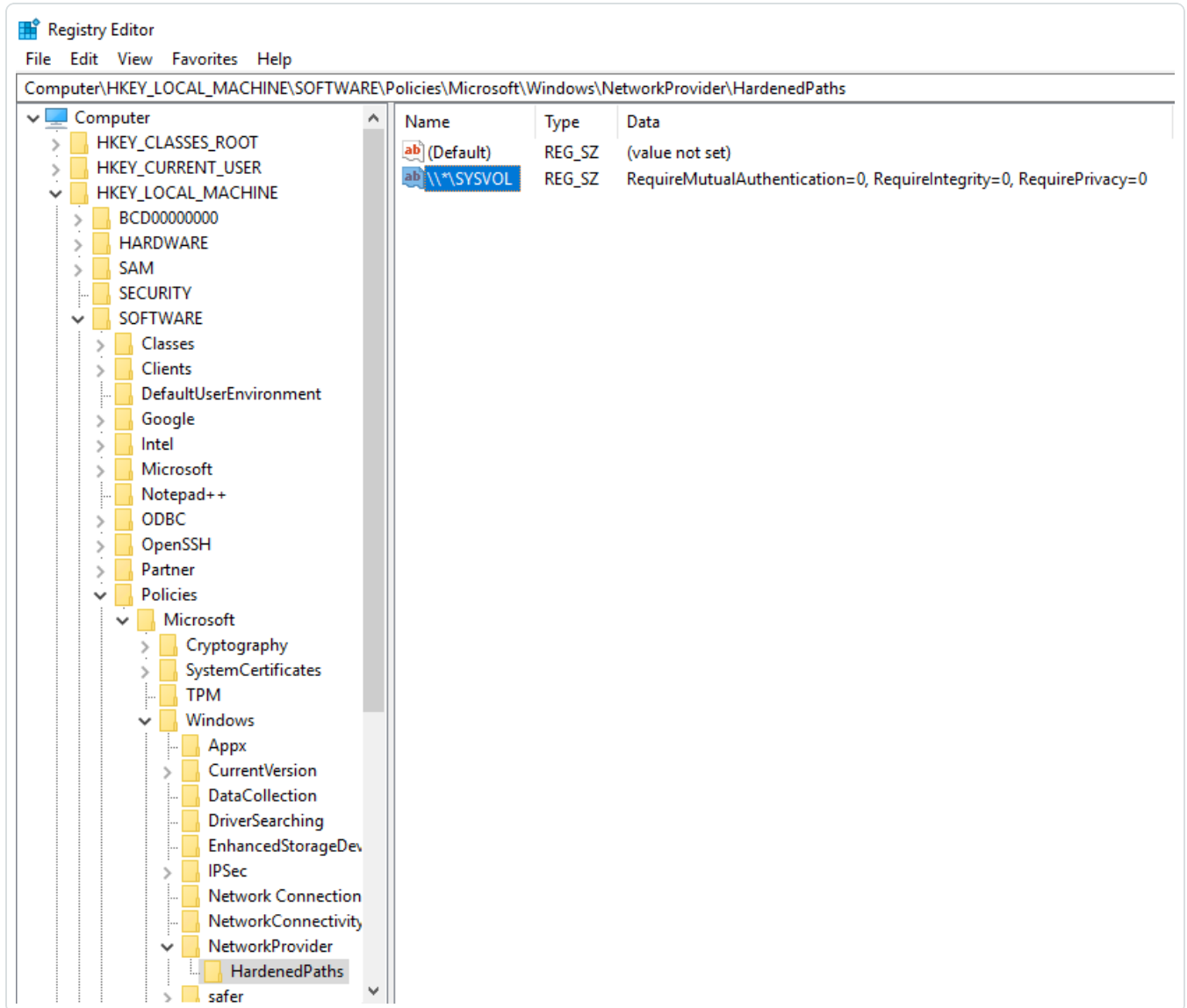
- b. En el campo "Nombre", escriba `*\SYSVOL`.

4. Haga doble clic en la clave `*\SYSVOL` (recién creada o ya existente) para abrir la ventana **Editar cadena**.



5. En el campo de datos **Valor**, ingrese los siguientes valores:
RequireMutualAuthentication=0, RequireIntegrity=0 y RequirePrivacy=0.
6. Haga clic en **Guardar**.

El resultado debería ser el siguiente:



7. Reinicie la máquina.

Registro (PowerShell)

Para deshabilitar el endurecimiento de SYSVOL en el registro mediante PowerShell:



1. Recopile los valores actuales de las claves del registro de rutas de acceso UNC protegidas como referencia mediante este comando de PowerShell:

```
Get-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths"
```

2. Establezca el valor recomendado:

```
New-ItemProperty -Path  
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths" -Name "\\*\SYSVOL" -  
Value "RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0"
```

3. Reinicie la máquina.

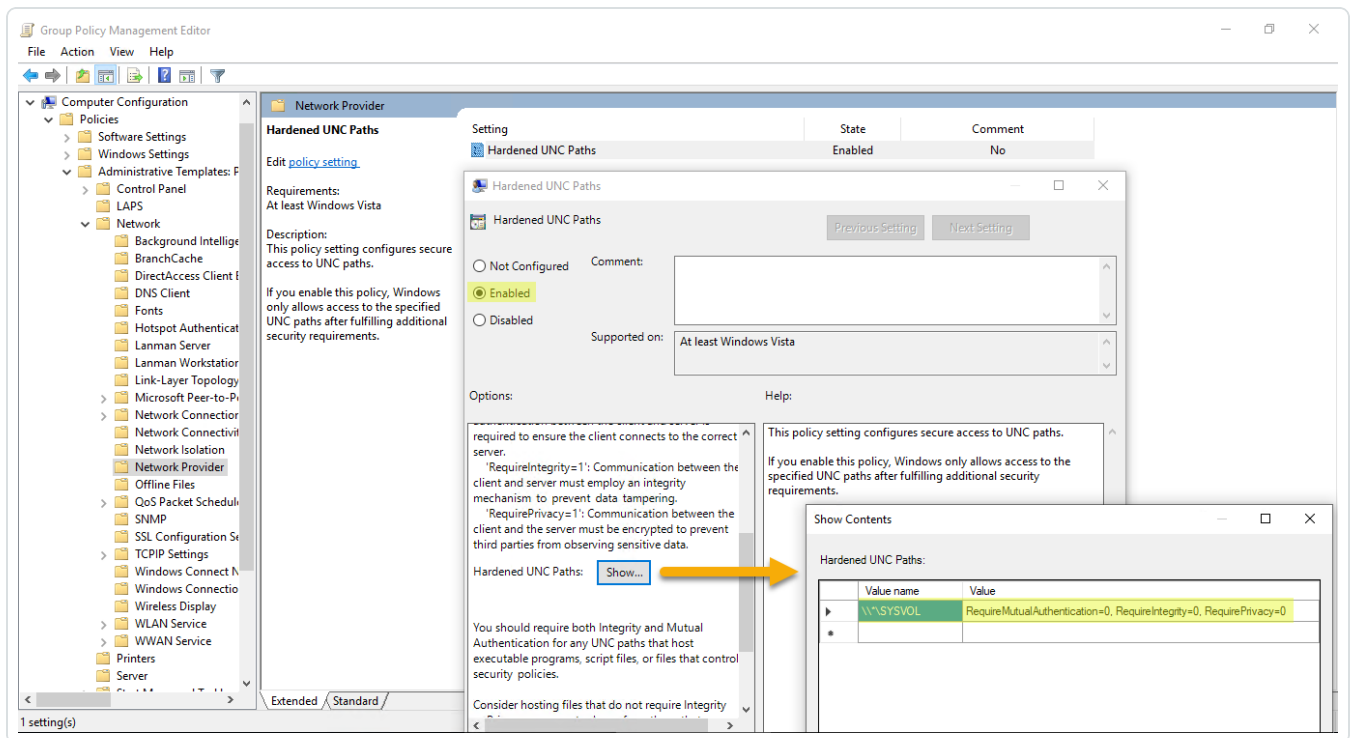
GPO

Requisito previo: Debe conectarse como usuario de Active Directory con los derechos para crear GPO en el dominio y vincularlos a la unidad organizativa que contiene la máquina de Directory Listener o Relay de Tenable Identity Exposure.

Para deshabilitar el endurecimiento de SYSVOL mediante un GPO:

1. Abra la Consola de administración de directivas de grupo.
2. Cree un nuevo GPO.
3. Edite el GPO y vaya a la siguiente ubicación: Configuración del equipo/Plantillas administrativas/Red/Proveedor de red/Rutas de acceso UNC protegidas.
4. Habilite esta opción y cree una nueva ruta de acceso UNC protegida con:
 - Nombre del valor = *\SYSVOL
 - Valor = RequireMutualAuthentication=0, RequireIntegrity=0 y RequirePrivacy=0.

El resultado debería ser el siguiente:

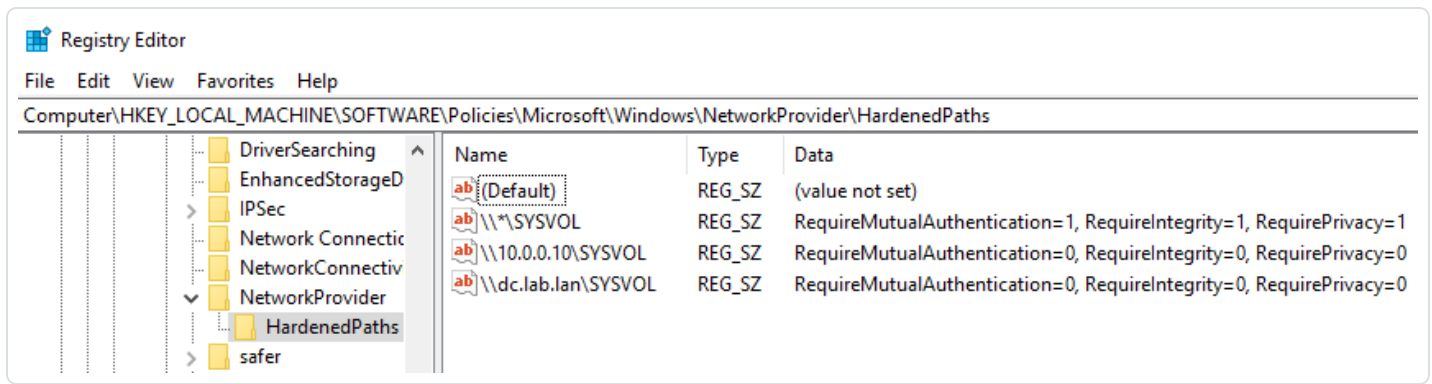


- Haga clic en **Aceptar** para confirmar.
- Vincule este GPO a la unidad organizativa que contiene la máquina de Directory Listener o Relay de Tenable Identity Exposure. También puede utilizar la funcionalidad del GPO de filtros de grupo de seguridad para garantizar que este GPO se aplique solo a esta máquina.

Excepciones de rutas de acceso UNC específicas

Los procedimientos anteriores deshabilitan el endurecimiento de SYSVOL mediante una ruta de acceso UNC comodín: "*\SYSVOL". También se puede deshabilitar solo para una dirección IP o FQDN en particular. Es decir, puede mantener habilitadas las opciones de rutas de acceso UNC protegidas (con el valor "1") para "*\SYSVOL" y tener una excepción correspondiente a cada dirección IP o FQDN de un controlador de dominio configurado en Tenable Identity Exposure.

En la siguiente imagen se muestra un ejemplo del endurecimiento de SYSVOL habilitado para todos los servidores ("*"), excepto "10.0.0.10" y "dc.lab.lan", que son controladores de dominio que configuramos en Tenable Identity Exposure:



Puede agregar estas opciones adicionales con los métodos de registro o GPO descritos anteriormente.

Nota: Tiene que especificar el valor exacto configurado en Tenable Identity Exposure (por ejemplo, no puede especificar una dirección IP si la configuración de Tenable Identity Exposure utiliza un FQDN). Además, recuerde actualizar estas claves cada vez que cambie una dirección IP o FQDN en la página de gestión de dominios de Tenable Identity Exposure.

Riesgos al deshabilitar el endurecimiento de SYSVOL

El endurecimiento de SYSVOL es una funcionalidad de seguridad y deshabilitarlo puede generar inquietudes válidas.

- Máquinas no unidas a un dominio: no existe ningún riesgo al deshabilitar el endurecimiento de SYSVOL. Dado que estas máquinas no aplican los GPO, no obtienen contenido del recurso compartido de SYSVOL para ejecutarlo.
- Máquinas unidas a un dominio (máquina de Directory Listener o Relay), que Tenable Identity Exposure **no recomienda**: si existe un riesgo potencial de que haya un atacante en una situación de tipo “Man in the middle” entre la máquina de Directory Listener o Relay y los controladores de dominio, no es seguro deshabilitar el endurecimiento de SYSVOL. En este caso, Tenable Identity Exposure recomienda que cambie a la autenticación de Kerberos.

El ámbito de esta desactivación se limita únicamente a la máquina de Directory Listener o Relay y no a otros equipos del dominio, y jamás a los controladores de dominio.