Configuración de la aplicación Cloud Security para IBM QRadar

Contenido

Introducción

Este documento describe cómo configurar la aplicación Cisco Cloud Security con IBM QRadar para el análisis de registros.

Overview

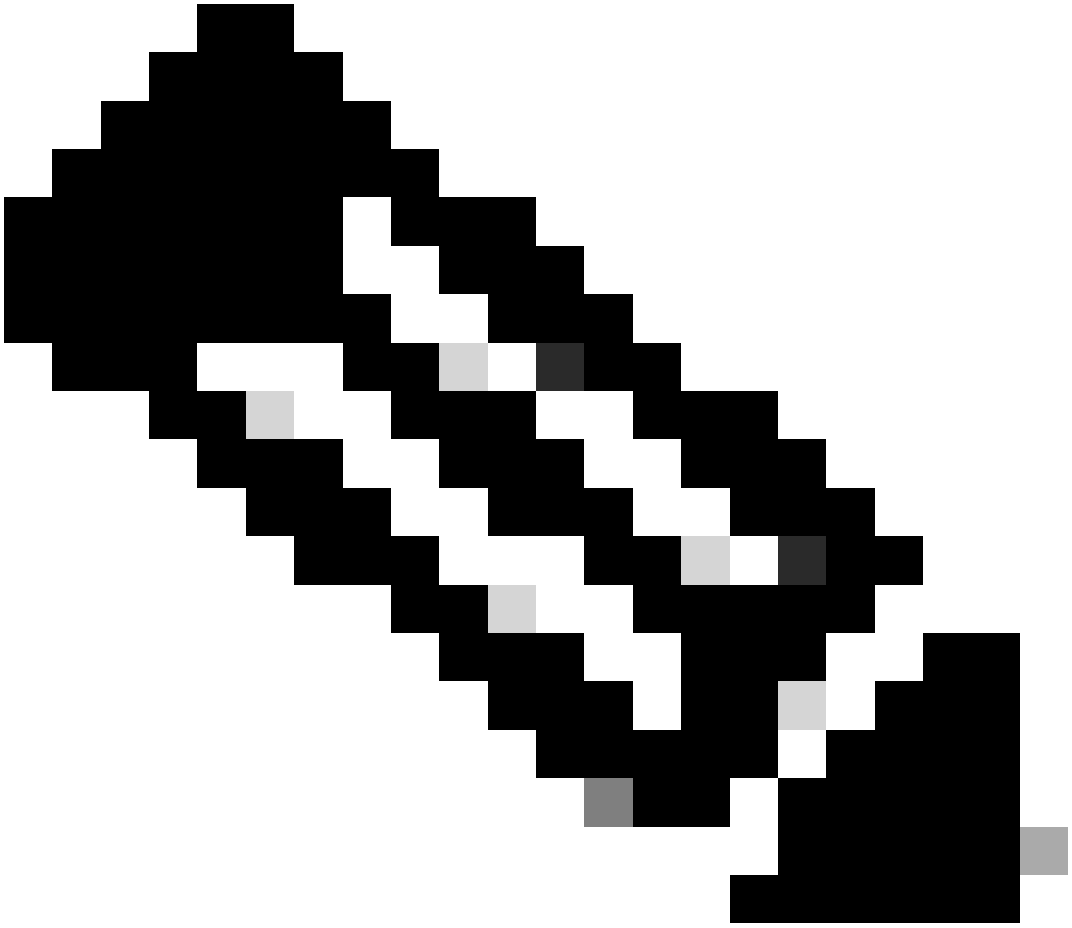
QRadar de IBM es un popular SIEM para el análisis de registros. Proporciona una interfaz potente para analizar grandes fragmentos de datos, como los registros proporcionados por Cisco Umbrella para el tráfico DNS de su organización. La aplicación Cisco Cloud Security App para IBM QRadar proporciona información de diversos productos de seguridad (Investigate, Enforcement y CloudLock) y los integra con QRadar. También ayuda al usuario a automatizar la seguridad y contener las amenazas más rápido y directamente desde QRadar.

Al configurar la aplicación Cisco Cloud Security para QRadar, integra todos los datos de la plataforma Cisco Cloud Security y le permite ver los datos en forma gráfica en la consola de QRadar. Desde la aplicación, los analistas pueden:

- Investigue dominios, direcciones IP y direcciones de correo electrónico
- Bloquear y desbloquear dominios (aplicación)
- Ver la información de todos los incidentes de la red.

Este artículo describe los procedimientos básicos para configurar y ejecutar QRadar de modo que sea capaz de extraer los registros de su cubeta S3 y consumirlos.

Requirements



Nota: El soporte para QRadar debe proceder de IBM, ya que Cisco no puede ofrecer soporte directo para hardware o software de terceros. Para cualquier problema de conexión de su panel de Umbrella a su cubeta S3, podemos proporcionar soporte. Gran parte de la información que se encuentra aquí también se puede encontrar en el sitio web de IBM: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umb

Requisitos generales de Cisco

Este documento asume que su cubeta Amazon AWS S3 se ha configurado en Umbrella (Configuración > Administración de registro) y se muestra en verde con los registros recientes que se han cargado.

Para obtener más información sobre cómo configurar esta función, lea aquí: Manage Your Logs.

Requisitos de IBM Security QRadar SIEM

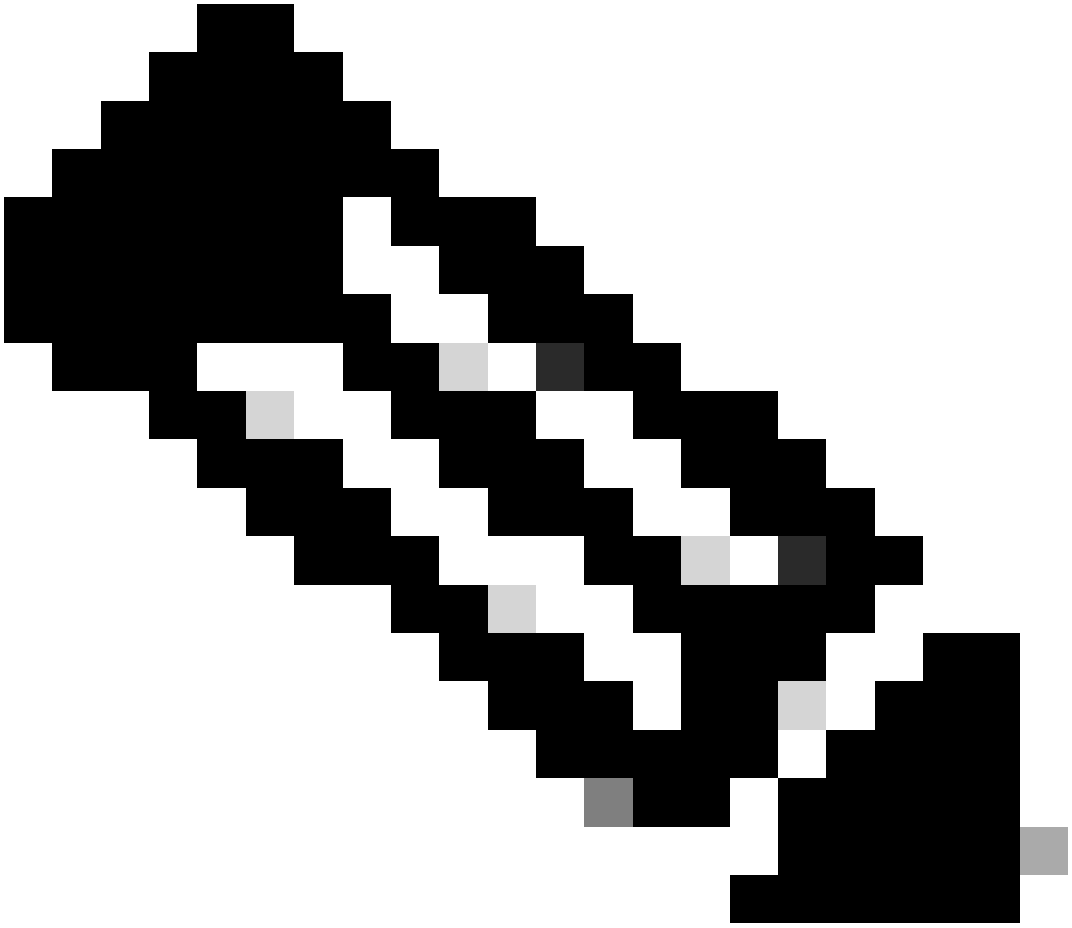
El administrador debe tener derechos administrativos sobre los dispositivos QRadar, la configuración de Amazon S3 y el panel de Umbrella. En estas instrucciones se asume que el administrador de QRadar está familiarizado con la creación de archivos LSX (Extensión de origen de registro).

Tenga en cuenta que Cisco Cloud Security App v1.0.3 solo funciona con IBM QRadar 7.2.8. La nueva versión, v1.0.6, funciona con la versión actual de QRadar de 7.4.2 y posteriores.

Instalación de Cisco Cloud Security App para IBM QRadar

1. Descargue e instale la aplicación Cisco Cloud Security App para IBM QRadar que se encuentra aquí: Cisco Cloud Security App v1.0.3 (para IBM QRadar v7.2.8) o Cisco Cloud Security App v1.0.6 (para IBM QRadar v7.4.8).
2. Después de la instalación, implemente los cambios en QRadar.

Configuración de la aplicación Cisco Cloud Security: Adición de origen de registro



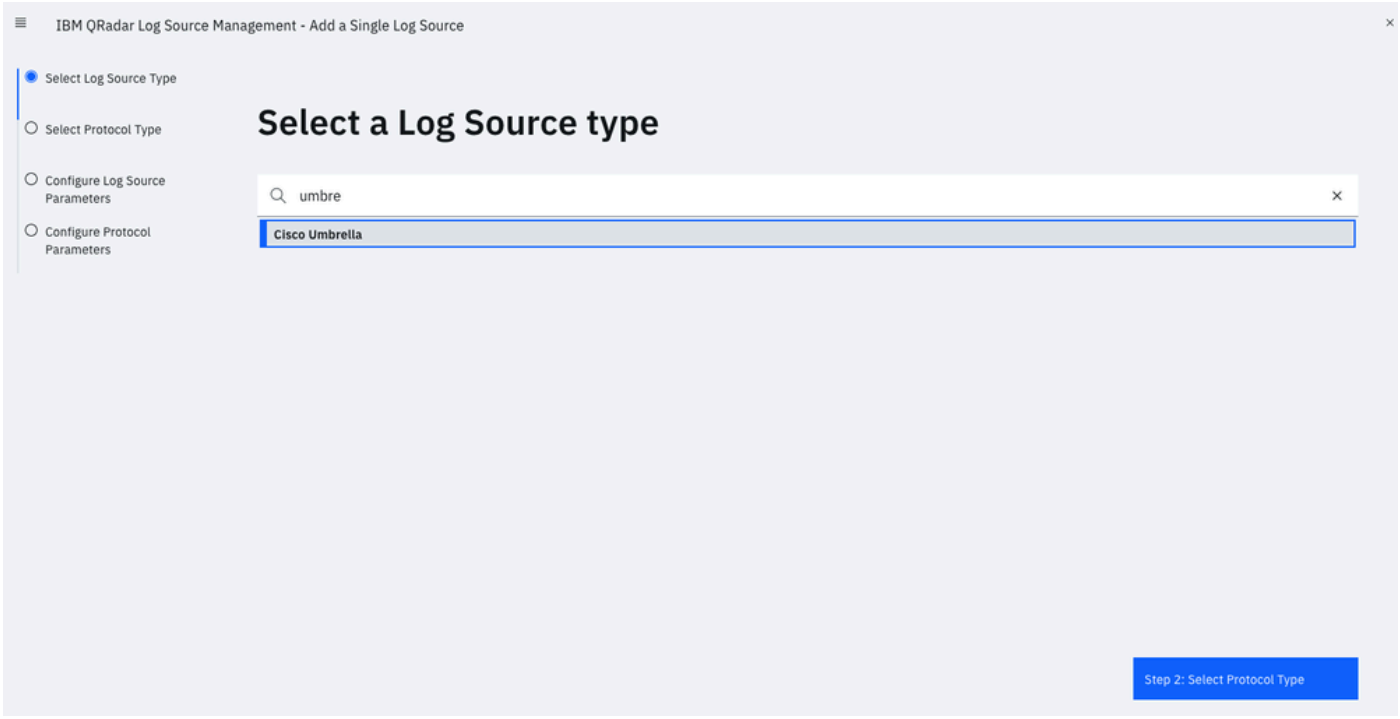
Nota: Puede ver otros registros en S3 como Audit y Firewall, pero no son compatibles. Configure sólo las tres que aparecen aquí. Cualquier intento de configurar esos otros registros produce un error.

Para agregar un origen de registro, haga clic en la pestaña Admin en la barra de navegación de QRadar, desplácese hacia abajo y haga clic en QRadar Log Source Management, luego haga clic en el botón +New Log Source:

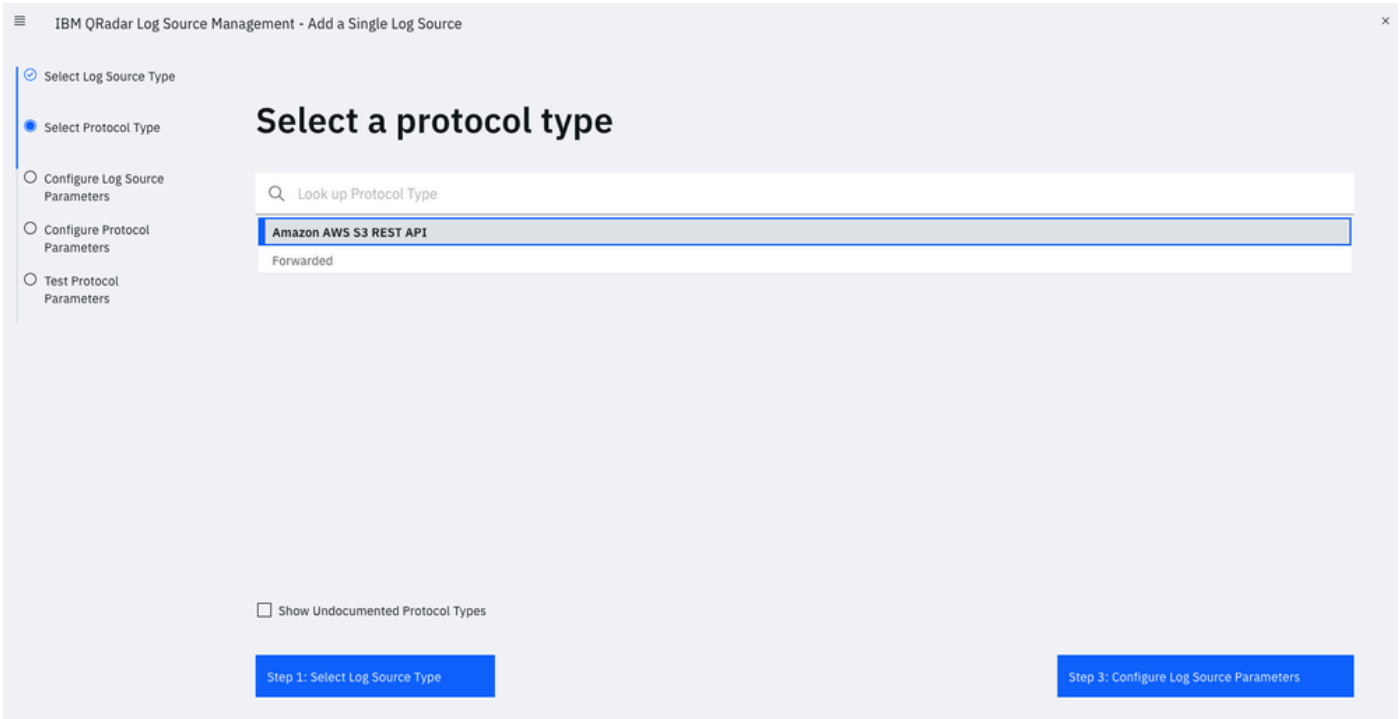
- Nombre de origen de registro (los nombres de entrada deben coincidir exactamente como se indica):
  - Registros de DNS de Cisco: cisco_umbrella_dns_logs
  - Registros de IP de Cisco Umbrella: cisco_umbrella_ip_logs
  - Registros de proxy de Cisco Umbrella: cisco_umbrella_proxy_logs
- Formato de evento: CSV de Cisco Umbrella
- Tipo de origen de registro: Cisco Umbrella
- Configuración de protocolos: API REST S3 de Amazon AWS
- Patrón de archivo: .*?\.csv\.gz

- Extensión de origen de registro: CiscoUmbrella_ext **
- Seleccione los grupos de los que desee que sea miembro este origen de registro: cisco_umbrella_logsource_group

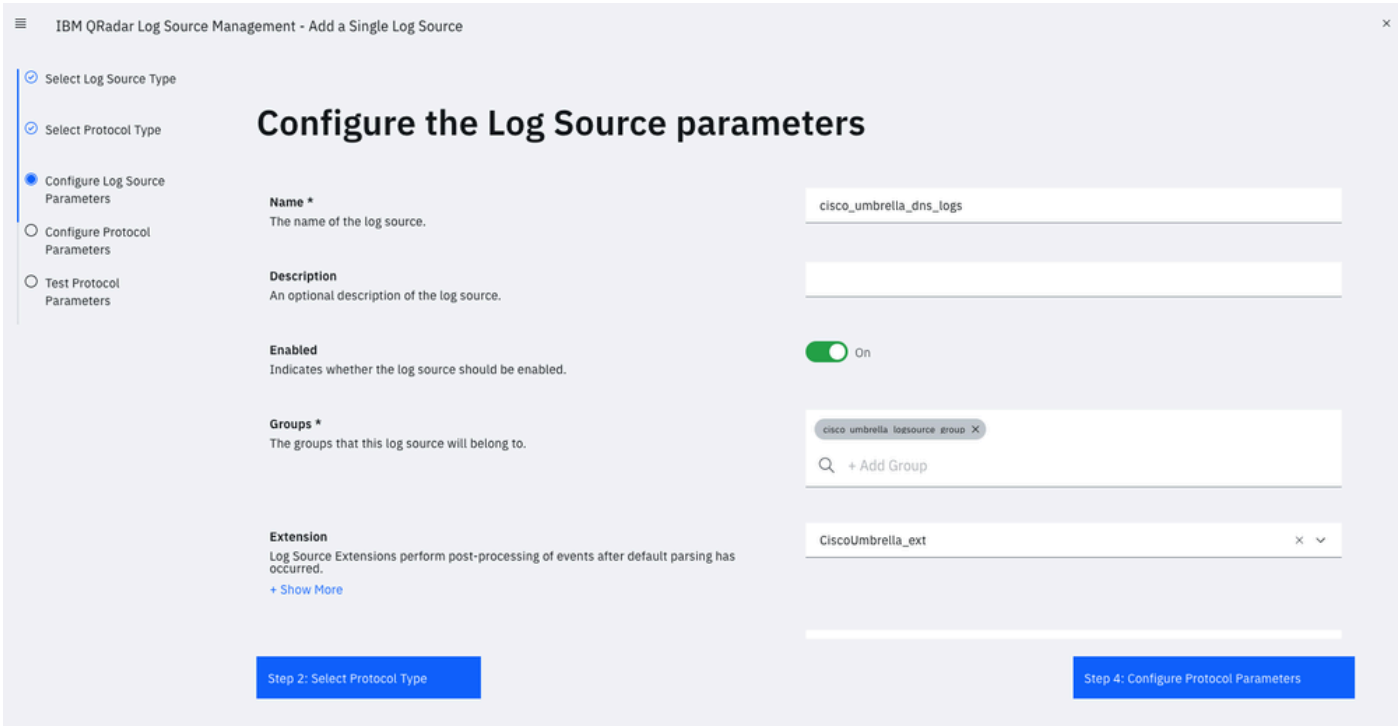
Vaya al Asistente para agregar un único origen de registro:



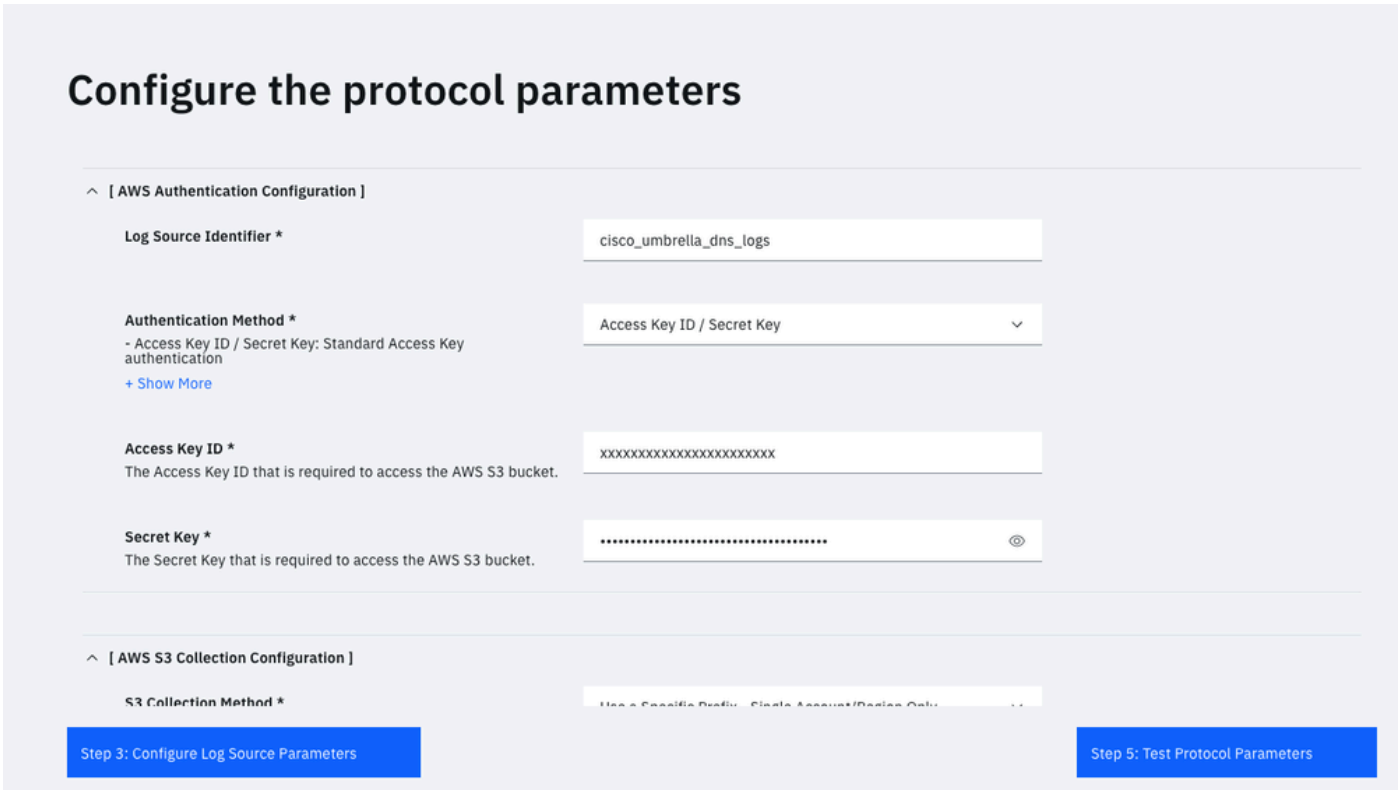
4404306773524



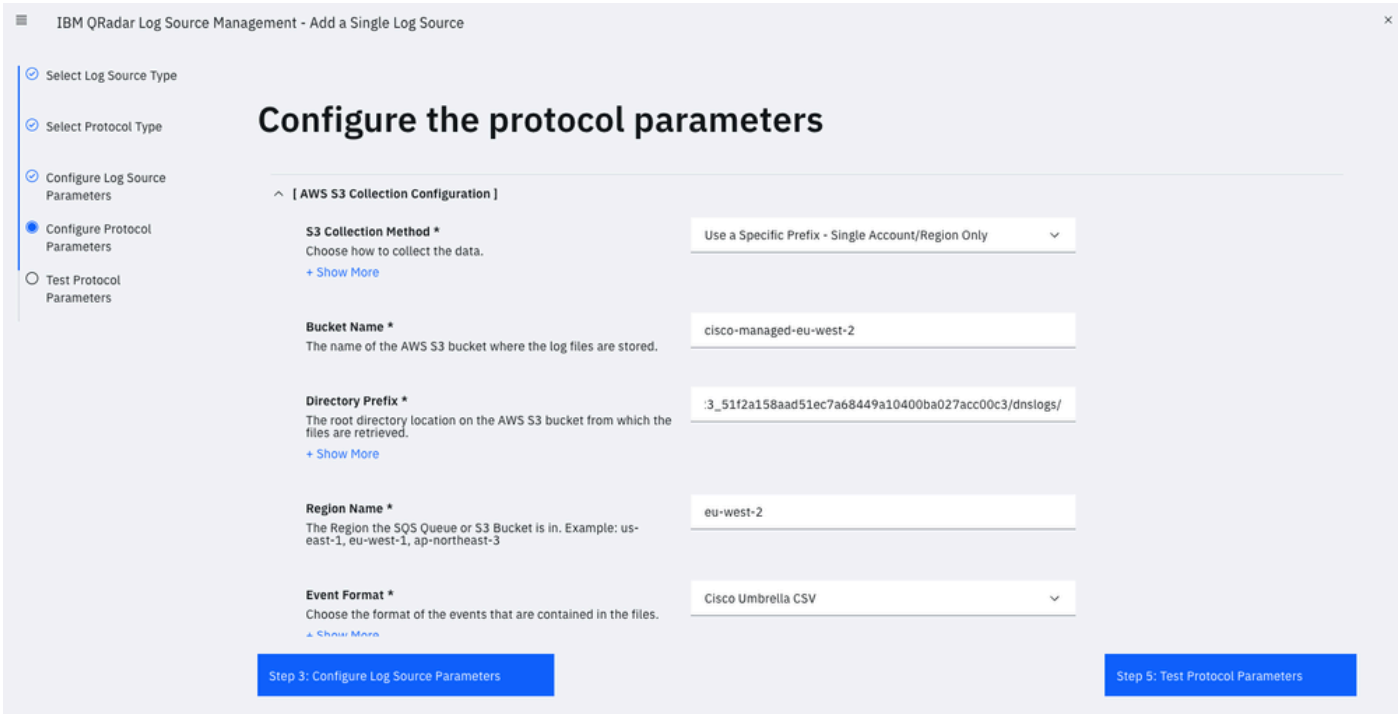
4404306773268



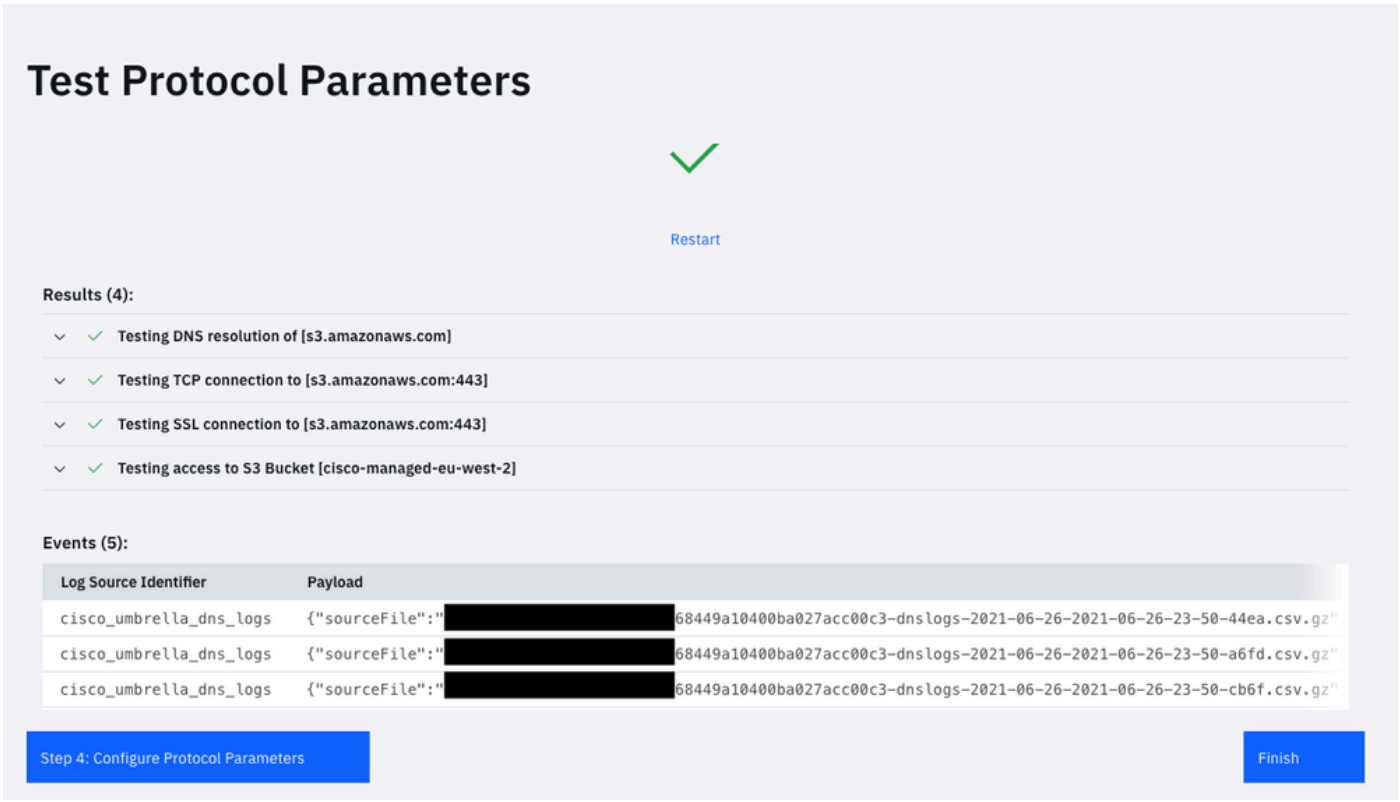
4404313505300



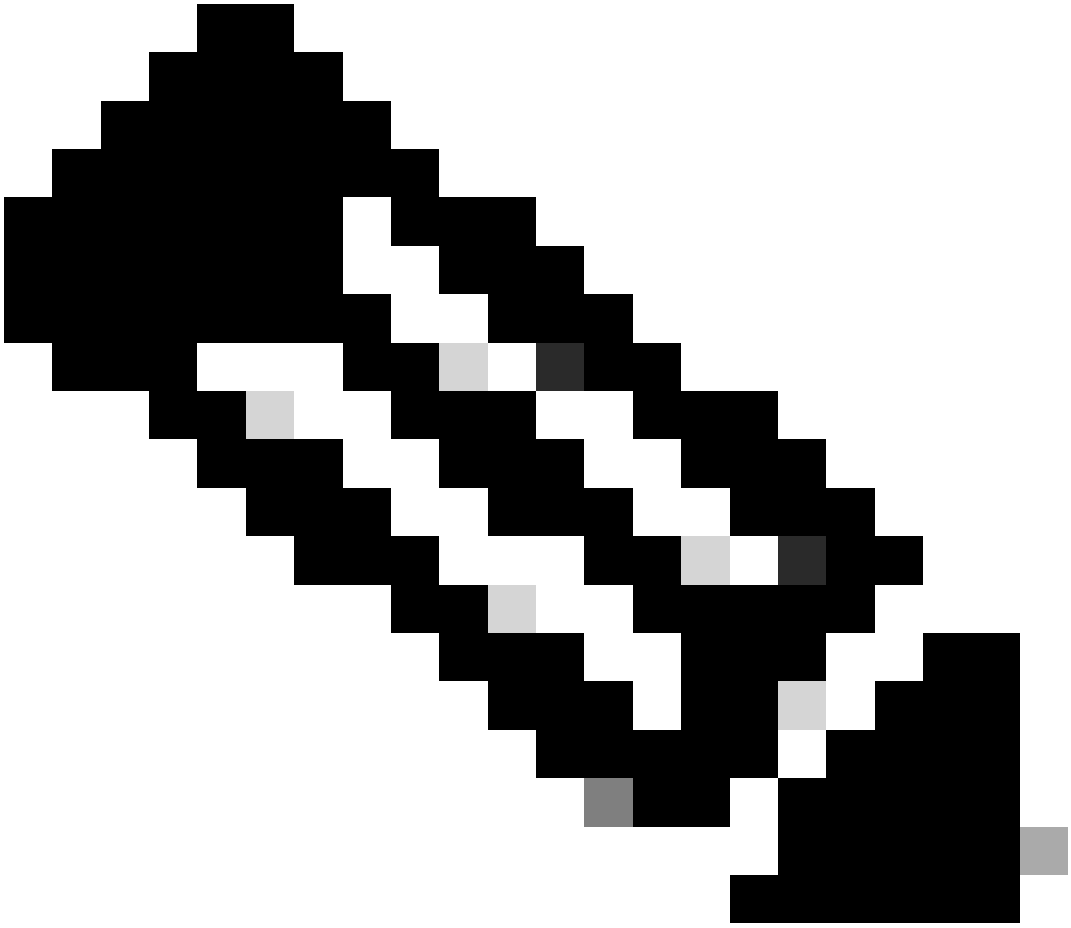
4404306774164



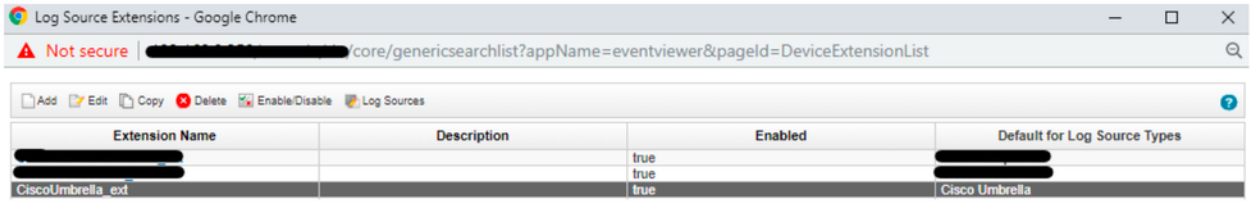
4404306897556



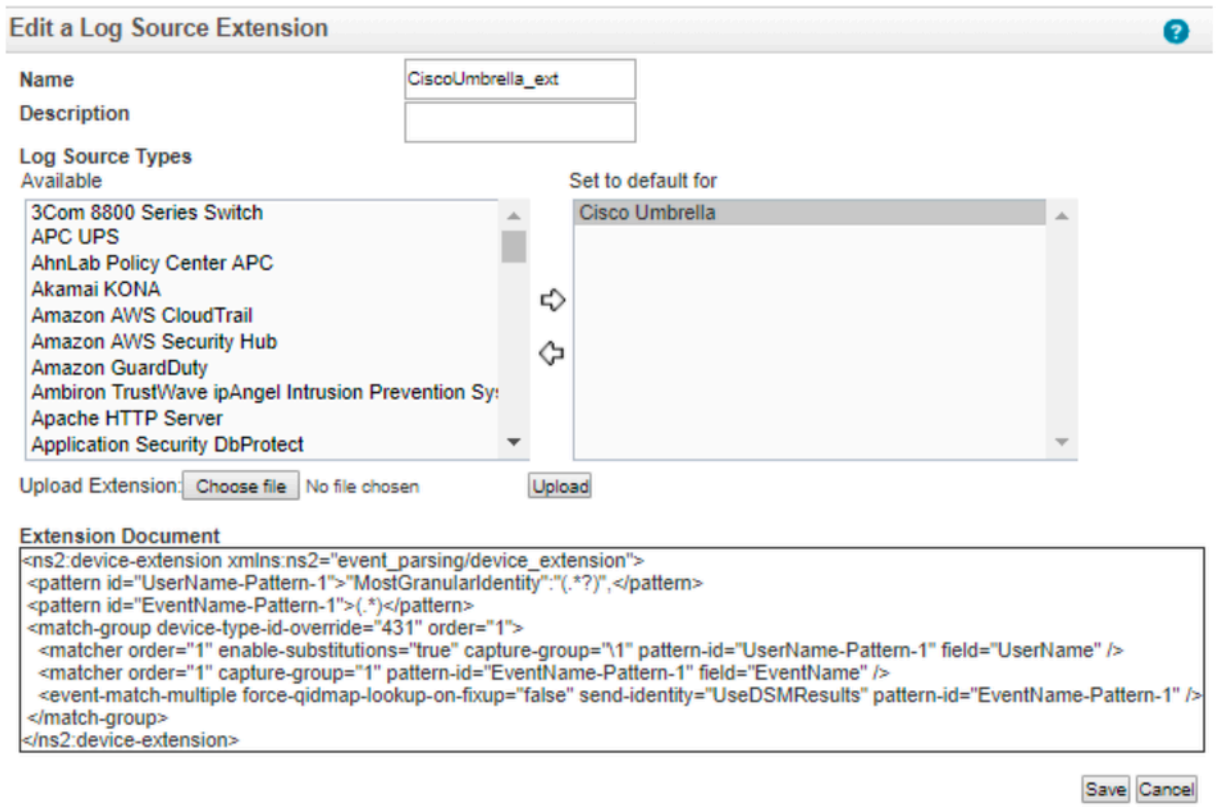
4404306881812



Nota: Si la extensión de origen de registro no está asignada a "CiscoUmbrella_ext", elija el nombre de origen de registro de la lista:



360071157752



360071326791

A continuación se muestra un ejemplo de cómo es un Cisco Managed Bucket:

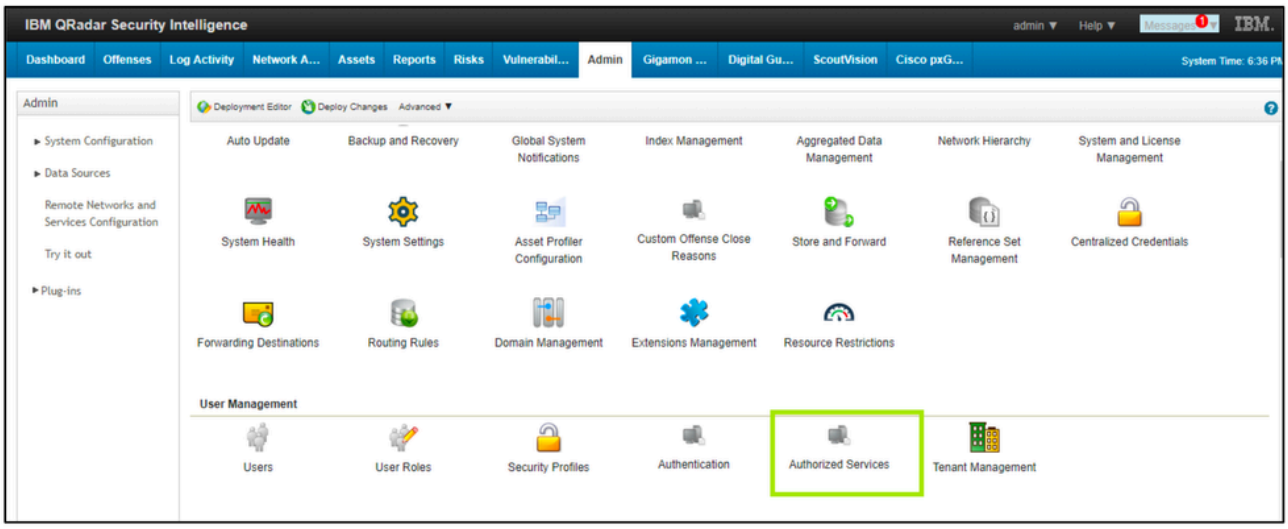
```
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxxx/dnslogs
```

Navegue hasta Cisco Cloud Security App Settings y establezca la frecuencia de actualización del panel en horas a un valor mínimo de "1" para que los gráficos muestren datos.

Generando token de autenticación

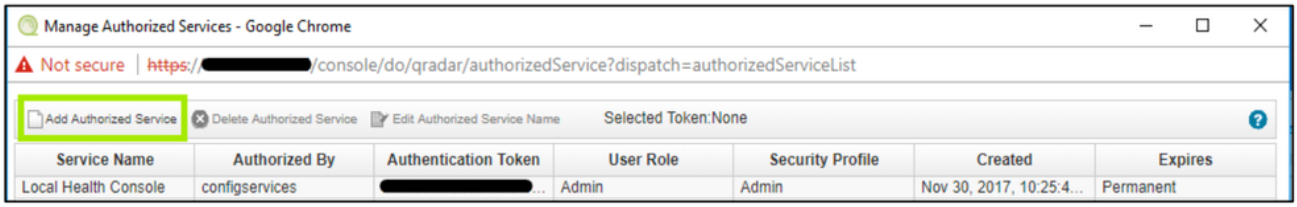
El administrador debe generar un token de servicio para agregarlo a la aplicación de seguridad de Cisco. Como práctica recomendada, se volvió a crear el token de servicio autorizado cada 90 días:

1. Inicie sesión en QRadar > Ficha Admin > Authorized Services.



360071965571

2. Agregue servicios autorizados.

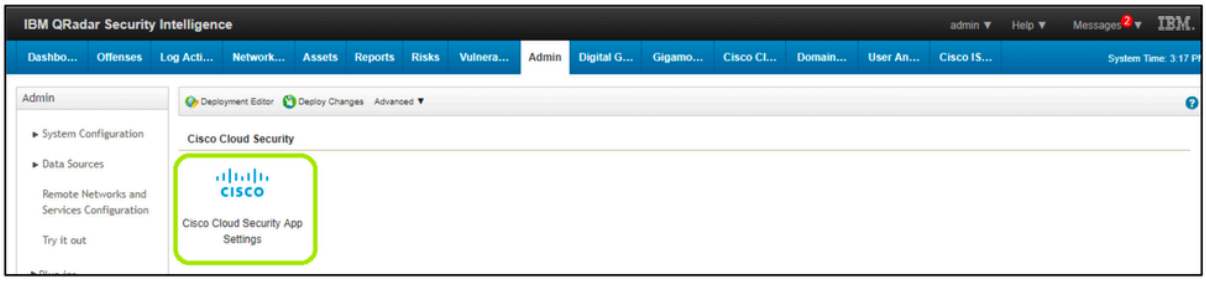


360071965551

3. Introduzca los detalles y genere el token de autenticación.
4. Después de generar el token, haga clic en "Implementar cambios".

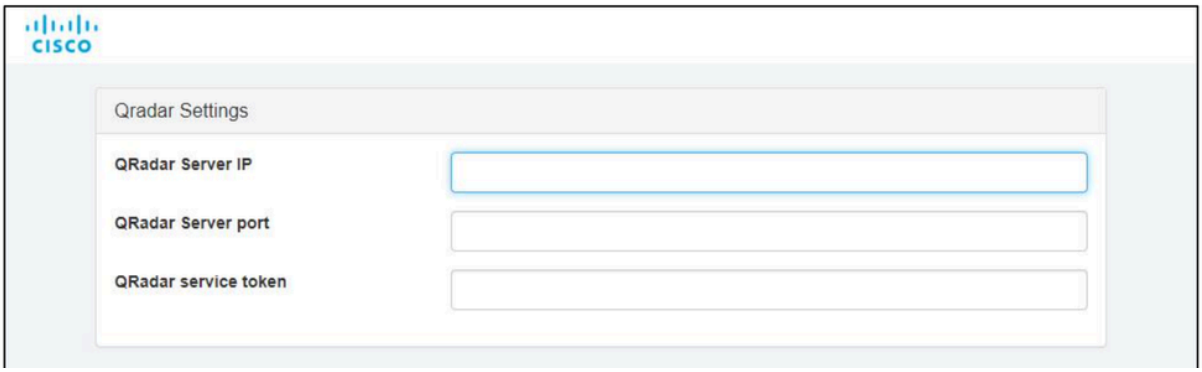
Configuración de la aplicación Cisco Cloud Security

1. En la pestaña Admin de la barra de navegación de QRadar, desplácese hacia abajo y abra Cisco Cloud Security App Settings.



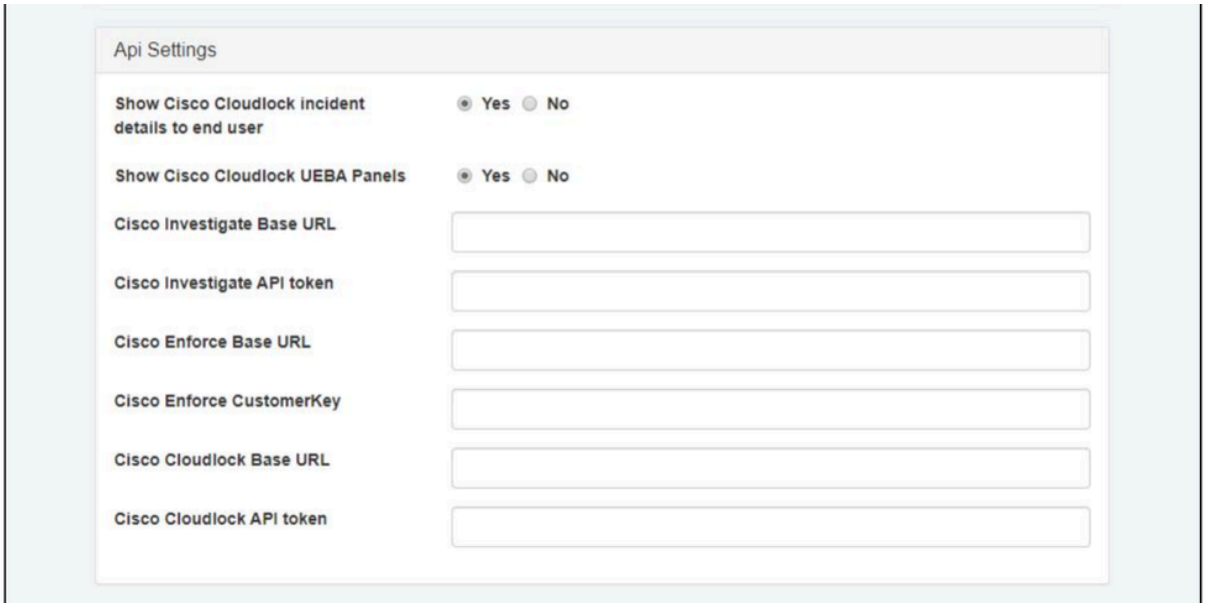
360071754732

2. Introduzca el token de autenticación generado en el paso anterior.



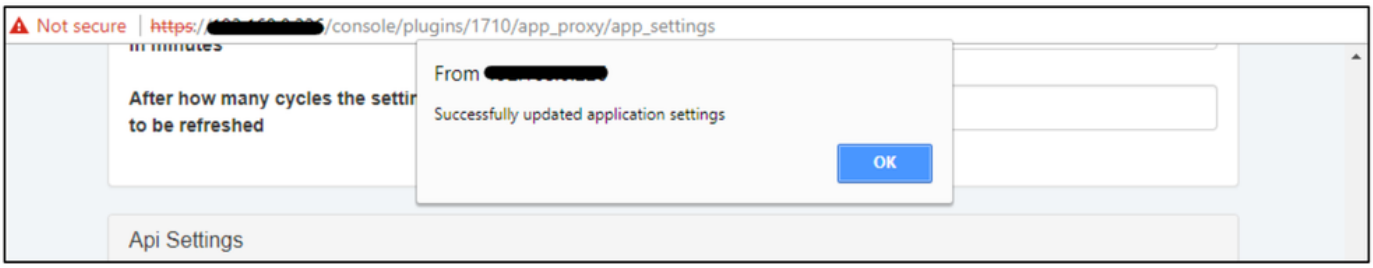
360072462992

3. Edite la Configuración de Api de la siguiente manera:
    - URL de base de investigación de Cisco: https://investigate.api.umbrella.com/
    - Token API de Cisco Investigate: generar mediante el panel de Umbrella -> Investigar -> Claves de API -> Crear nuevo token; para obtener más información, consulte https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key
    - URL de base de aplicación de Cisco: https://s-platform.api.opendns.com/1.0/
    - Cisco Enforce CustomerKey: generar mediante el panel de control general -> Componentes de la política -> Integraciones -> Agregar; para obtener más información, consulte https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations
    - URL base de Cisco Cloudlock: https://{YourCloudlockAPIServer}/api/v2 (por ejemplo, https://api-demo.cloudlock.com/api/v2/. Confirme la URL de la base Cloudlock (también denominada URL de la API Cloudlock Enterprise) enviando un correo electrónico a support@cloudlock.com.)
    - Token API de Cisco Cloudlock: generar mediante Cloudlock -> Configuración -> Autenticación y API -> Generar; para obtener más información, consulte https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication



360072703611

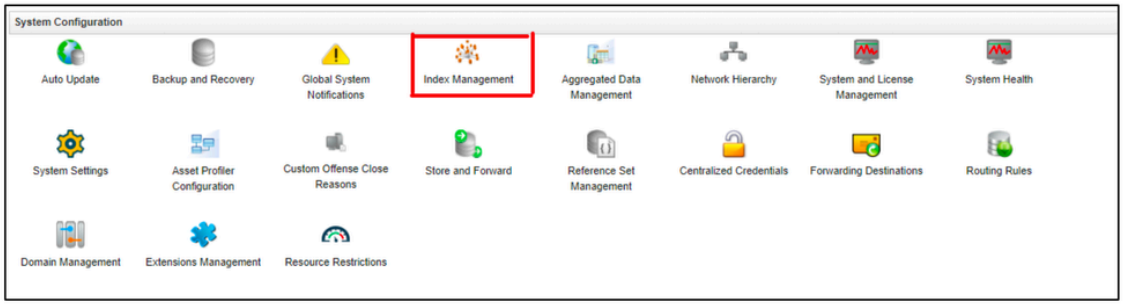
Una ventana emergente indica que la configuración de la aplicación se ha actualizado correctamente.



360071986151

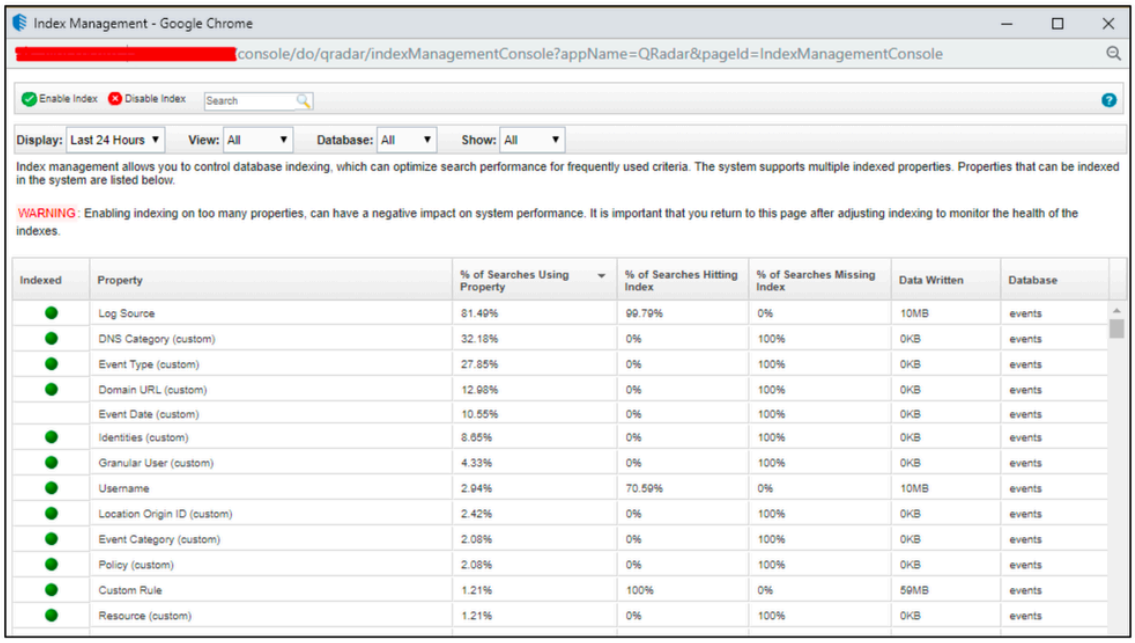
Indexación en QRadar

1. Navegue hasta la pestaña Admin, luego haga clic en Index Management.



360071780112

2. Indizar los CEP empaquetados con la aplicación.



360071988811

Estos son los CEP recomendados para indexar:

1. Origen de registro
2. Categoría de DNS
3. Tipo de Evento
4. URL de dominio
5. Identidades
6. Usuario granular
7. Nombre de usuario
8. ID de origen de ubicación
9. Categoría de evento
10. Política
11. Recurso

Ahora está listo para usar QRadar para comenzar a supervisar las actividades relacionadas con los detalles de Cisco Umbrella, Investigate y CloudLock. Puede encontrar más instrucciones sobre cómo navegar por QRadar aquí: Navegación por la aplicación Cisco Cloud Security.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).