

Configuración de la aplicación Cloud Security para IBM QRadar

Contenido

[Introducción](#)

[Overview](#)

[Requirements](#)

[Requisitos generales de Cisco](#)

[Requisitos de IBM Security QRadar SIEM](#)

[Instalación de Cisco Cloud Security App para IBM QRadar](#)

[Configuración de la aplicación Cisco Cloud Security: Adición de origen de registro](#)

[Generando token de autenticación](#)

[Configuración de la aplicación Cisco Cloud Security](#)

[Indexación en QRadar](#)

Introducción

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

Overview

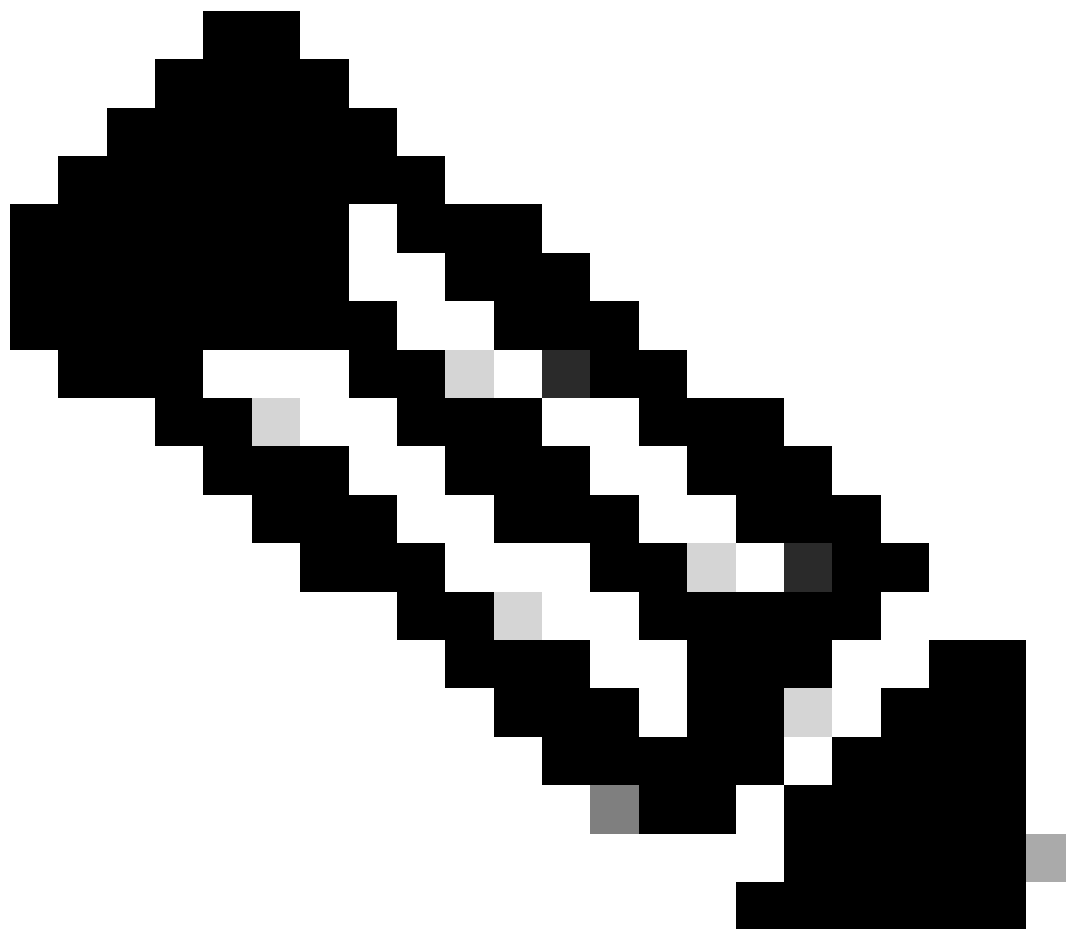
QRadar de IBM es un popular SIEM para el análisis de registros. Proporciona una interfaz potente para analizar grandes fragmentos de datos, como los registros proporcionados por Cisco Umbrella para el tráfico DNS de su organización. La aplicación Cisco Cloud Security App para IBM QRadar proporciona información 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_Umbrella.html

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

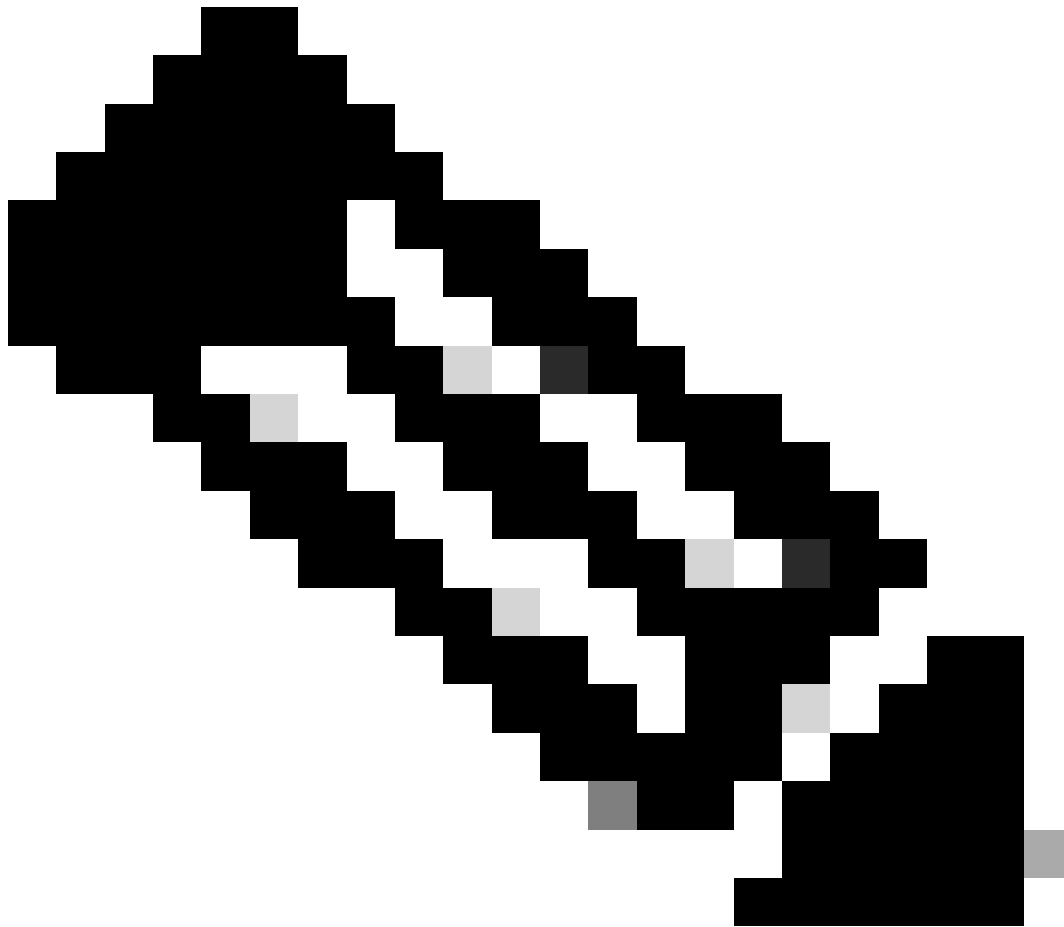
El administrador debe tener derechos administrativos sobre los dispositivos QRadar, la configuración de Amazon S3 y el panel de Umbrella. En estas instrucciones se asume que el administrador de QRadar está familiarizado con la creación de archivos LSX (Extensión de origen de registro).

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:

The screenshot shows the 'Select a Log Source type' screen. On the left, a sidebar lists the steps: 'Select Log Source Type' (selected), 'Select Protocol Type', 'Configure Log Source Parameters', and 'Configure Protocol Parameters'. The main area has a search bar with the text 'umbre' and a dropdown menu showing 'Cisco Umbrella'. A blue button at the bottom right is labeled 'Step 2: Select Protocol Type'.

4404306773524

The screenshot shows the 'Select a protocol type' screen. The sidebar now has 'Select Protocol Type' selected. The main area has a search bar with the text 'Look up Protocol Type' and a dropdown menu showing 'Amazon AWS S3 REST API' and 'Forwarded'. A checkbox at the bottom left is labeled 'Show Undocumented Protocol Types'. Two blue buttons are at the bottom: 'Step 1: Select Log Source Type' on the left and 'Step 3: Configure Log Source Parameters' on the right.

4404306773268

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Test Protocol Parameters

Configure the Log Source parameters

Name *

The name of the log source.

cisco_umbrella_dns_logs

Description

An optional description of the log source.

Enabled

Indicates whether the log source should be enabled.

On

Groups *

The groups that this log source will belong to.

cisco_umbrella_logsource_group

+ Add Group

Extension

Log Source Extensions perform post-processing of events after default parsing has occurred.

+ Show More

CiscoUmbrella_ext

Step 2: Select Protocol Type

Step 4: Configure Protocol Parameters

4404313505300

Configure the protocol parameters

[AWS Authentication Configuration]

Log Source Identifier *

cisco_umbrella_dns_logs

Authentication Method *

- Access Key ID / Secret Key: Standard Access Key authentication

+ Show More

Access Key ID / Secret Key

Access Key ID *

The Access Key ID that is required to access the AWS S3 bucket.

XXXXXXXXXXXXXXXXXXXX

Secret Key *

The Secret Key that is required to access the AWS S3 bucket.

.....

[AWS S3 Collection Configuration]

S3 Collection Method *

Use a Specific Profile (Single Account/Region Only)

Step 3: Configure Log Source Parameters

Step 5: Test Protocol Parameters

4404306774164

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Test Protocol Parameters

Configure the protocol parameters

^ [AWS S3 Collection Configuration]

S3 Collection Method *

Choose how to collect the data.

+ Show More

Use a Specific Prefix - Single Account/Region Only

Bucket Name *

The name of the AWS S3 bucket where the log files are stored.

cisco-managed-eu-west-2

Directory Prefix *

The root directory location on the AWS S3 bucket from which the files are retrieved.

+ Show More

:3_51f2a158aad51ec7a68449a10400ba027acc00c3/dnslogs/

Region Name *

The Region the SQS Queue or S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3

eu-west-2

Event Format *

Choose the format of the events that are contained in the files.

+ Show More

Cisco Umbrella CSV

Step 3: Configure Log Source Parameters

Step 5: Test Protocol Parameters

4404306897556

Test Protocol Parameters

✓

Restart

Results (4):

✓ Testing DNS resolution of [s3.amazonaws.com]

✓ Testing TCP connection to [s3.amazonaws.com:443]

✓ Testing SSL connection to [s3.amazonaws.com:443]

✓ Testing access to S3 Bucket [cisco-managed-eu-west-2]

Events (5):

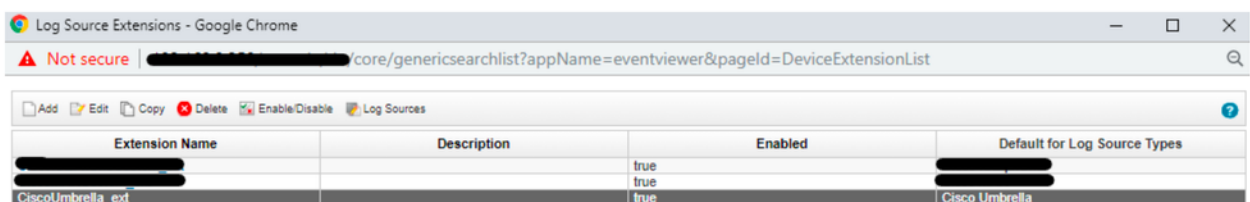
Log Source Identifier	Payload
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-44ea.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-a6fd.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile":"[REDACTED]68449a10400ba027acc00c3-dnslogs-2021-06-26-2021-06-26-23-50-cb6f.csv.gz"}

Step 4: Configure Protocol Parameters

Finish

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:



Extension Name	Description	Enabled	Default for Log Source Types
[Redacted]		true	[Redacted]
[Redacted]		true	[Redacted]
CiscoUmbrella_ext		true	Cisco Umbrella

360071157752

Edit a Log Source Extension

Name
CiscoUmbrella_ext

Description

Log Source Types

Available

3Com 8800 Series Switch
APC UPS
AhnLab Policy Center APC
Akamai KONA
Amazon AWS CloudTrail
Amazon AWS Security Hub
Amazon GuardDuty
Ambion TrustWave ipAngel Intrusion Prevention Sy
Apache HTTP Server
Application Security DbProtect

Set to default for

Cisco Umbrella

Upload Extension: Choose file No file chosen Upload

Extension Document

<ns2:device-extension xmlns:ns2="event_parsing/device_extension">
<pattern id="UserName-Pattern-1">"MostGranularIdentity": "(.*)", </pattern>
<pattern id="EventName-Pattern-1">(.*)</pattern>
<match-group device-type-id-override="431" order="1">
<matcher order="1" enable-substitutions="true" capture-group="1" pattern-id="UserName-Pattern-1" field="UserName" />
<matcher order="1" capture-group="1" pattern-id="EventName-Pattern-1" field="EventName" />
<event-match-multiple force-qidmap-lookup-on-fixup="false" send-identity="UseDSMResults" pattern-id="EventName-Pattern-1" />
</match-group>
</ns2:device-extension>

Save Cancel

360071326791

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

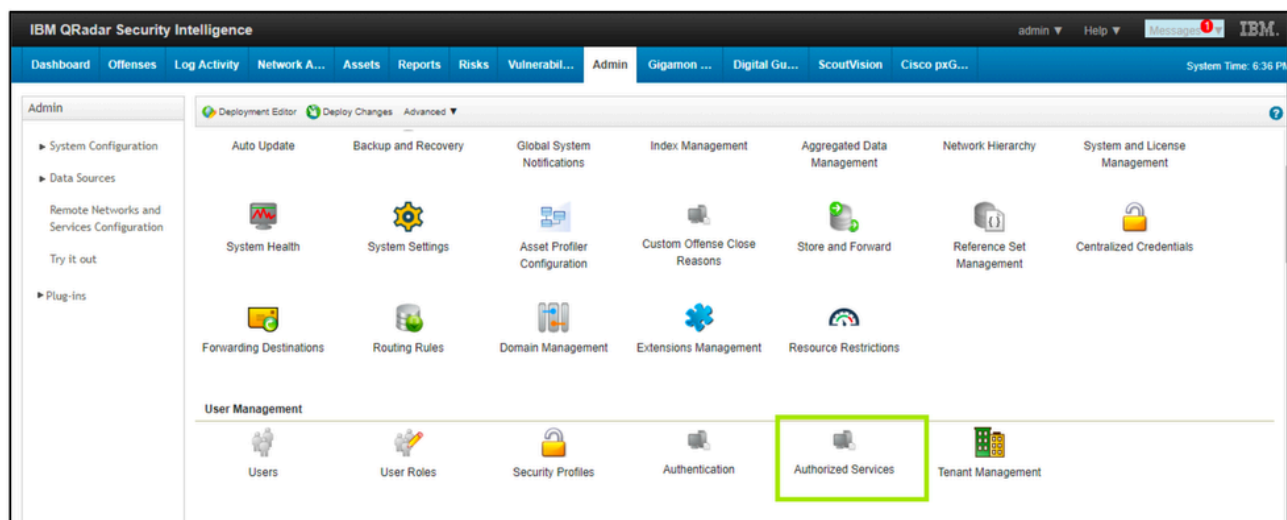
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxx/dnslogs

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

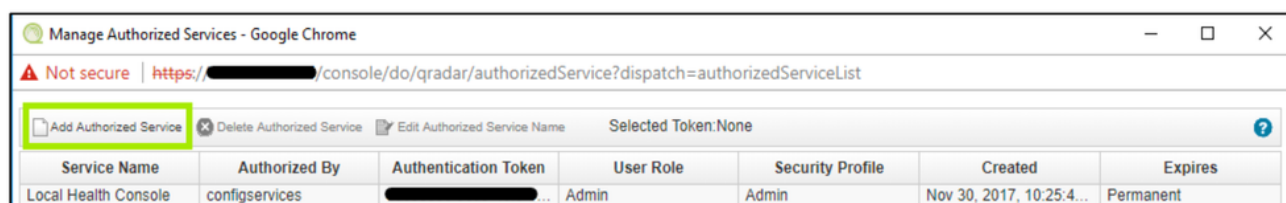
El administrador debe generar un token de servicio para agregarlo a la aplicación de seguridad de Cisco. Como práctica recomendada, se volvió a crear el token de servicio autorizado cada 90 días:

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



360071965571

2. Agregue servicios autorizados.



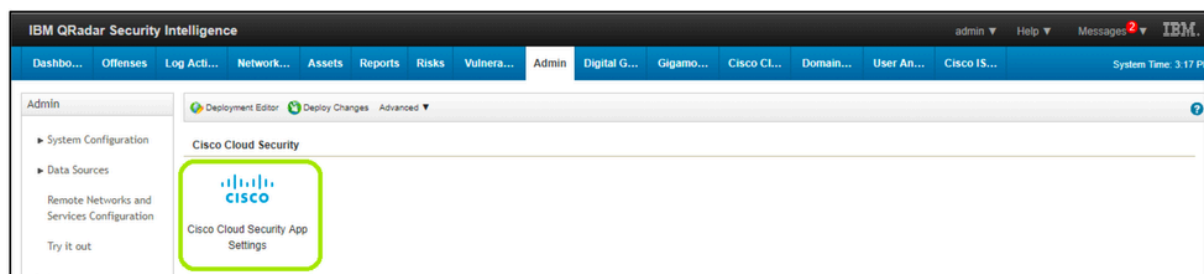
360071965551

3. Introduzca los detalles y genere el token de autenticación.

4. Después de generar el token, haga clic en "Implementar cambios".

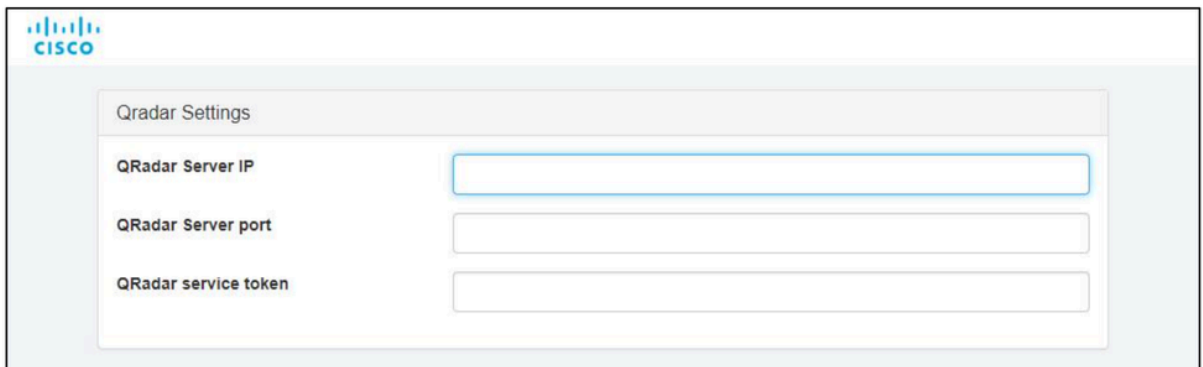
Configuración de la aplicación Cisco Cloud Security

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.



Qradar Settings

QRadar Server IP

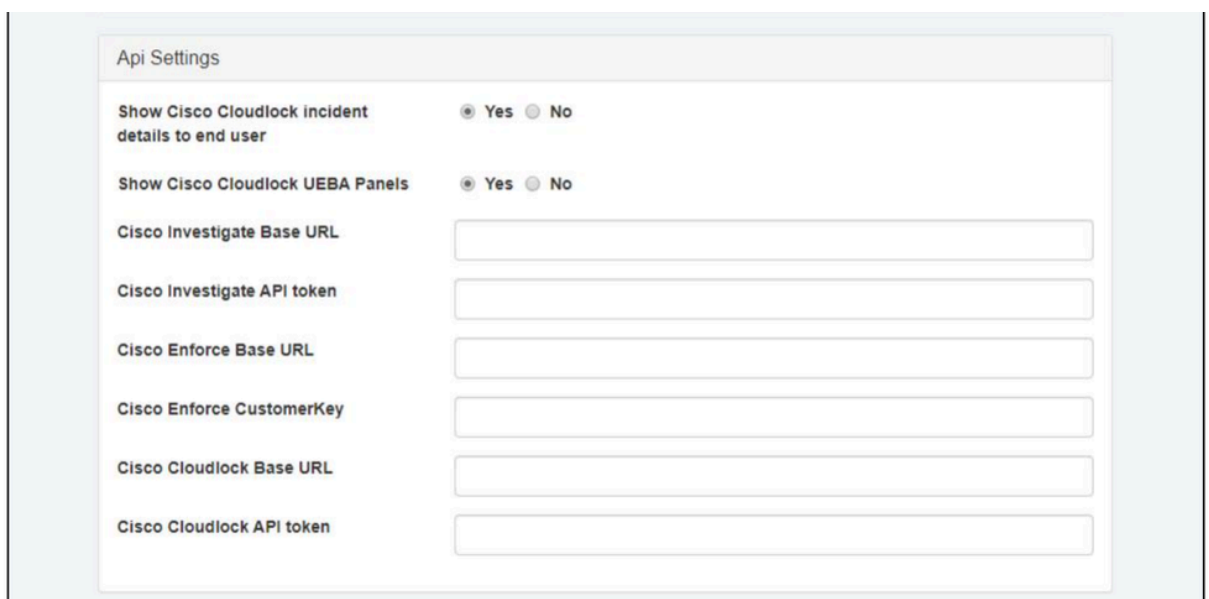
QRadar Server port

QRadar service token

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>



Api Settings

Show Cisco Cloudlock incident details to end user ☒ Yes ☐ No

Show Cisco Cloudlock UEBA Panels ☒ Yes ☐ No

Cisco Investigate Base URL

Cisco Investigate API token

Cisco Enforce Base URL

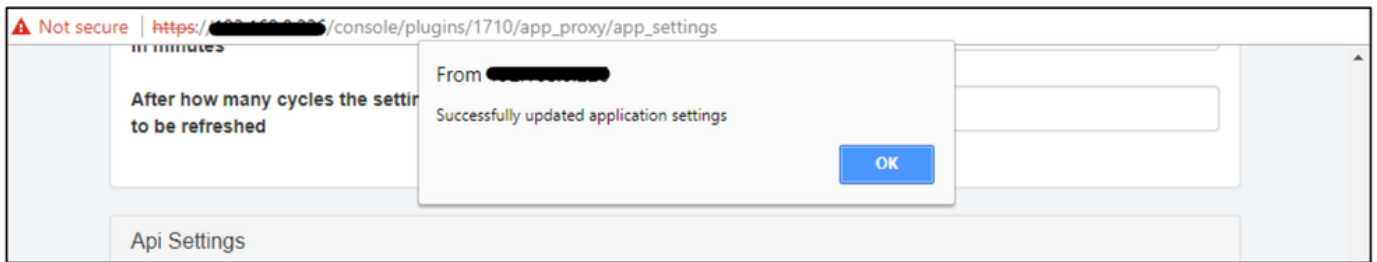
Cisco Enforce CustomerKey

Cisco Cloudlock Base URL

Cisco Cloudlock API token

360072703611

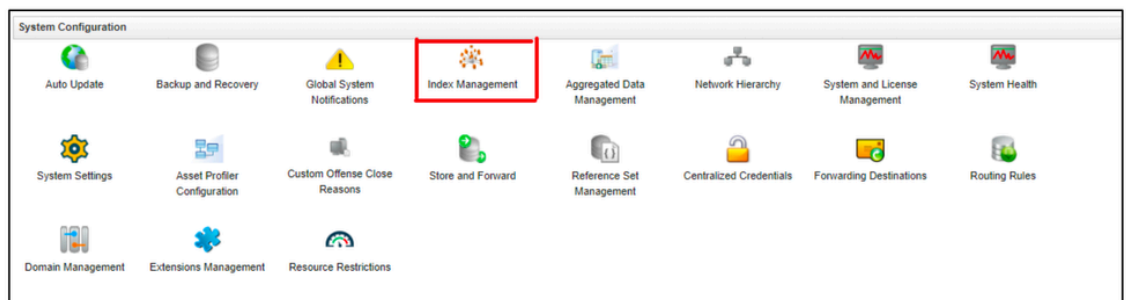
Una ventana emergente indica que la configuración de la aplicación se ha actualizado correctamente.



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.

Index Management - Google Chrome

console/do/qradar/indexManagementConsole?appName=QRadar&pageId=IndexManagementConsole

Enable Index Disable Index Search

Display: Last 24 Hours View: All Database: All Show: All

Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

WARNING: Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	Log Source	81.49%	99.79%	0%	10MB	events
●	DNS Category (custom)	32.18%	0%	100%	0KB	events
●	Event Type (custom)	27.85%	0%	100%	0KB	events
●	Domain URL (custom)	12.96%	0%	100%	0KB	events
●	Event Date (custom)	10.55%	0%	100%	0KB	events
●	Identities (custom)	8.65%	0%	100%	0KB	events
●	Granular User (custom)	4.33%	0%	100%	0KB	events
●	Username	2.94%	70.59%	0%	10MB	events
●	Location Origin ID (custom)	2.42%	0%	100%	0KB	events
●	Event Category (custom)	2.08%	0%	100%	0KB	events
●	Policy (custom)	2.08%	0%	100%	0KB	events
●	Custom Rule	1.21%	100%	0%	59MB	events
●	Resource (custom)	1.21%	0%	100%	0KB	events

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).