Configurar o aplicativo Cloud Security para IBM QRadar

Contents

Introdução

Este documento descreve como configurar o aplicativo Cisco Cloud Security com o IBM QRadar para análise de log.

Overview

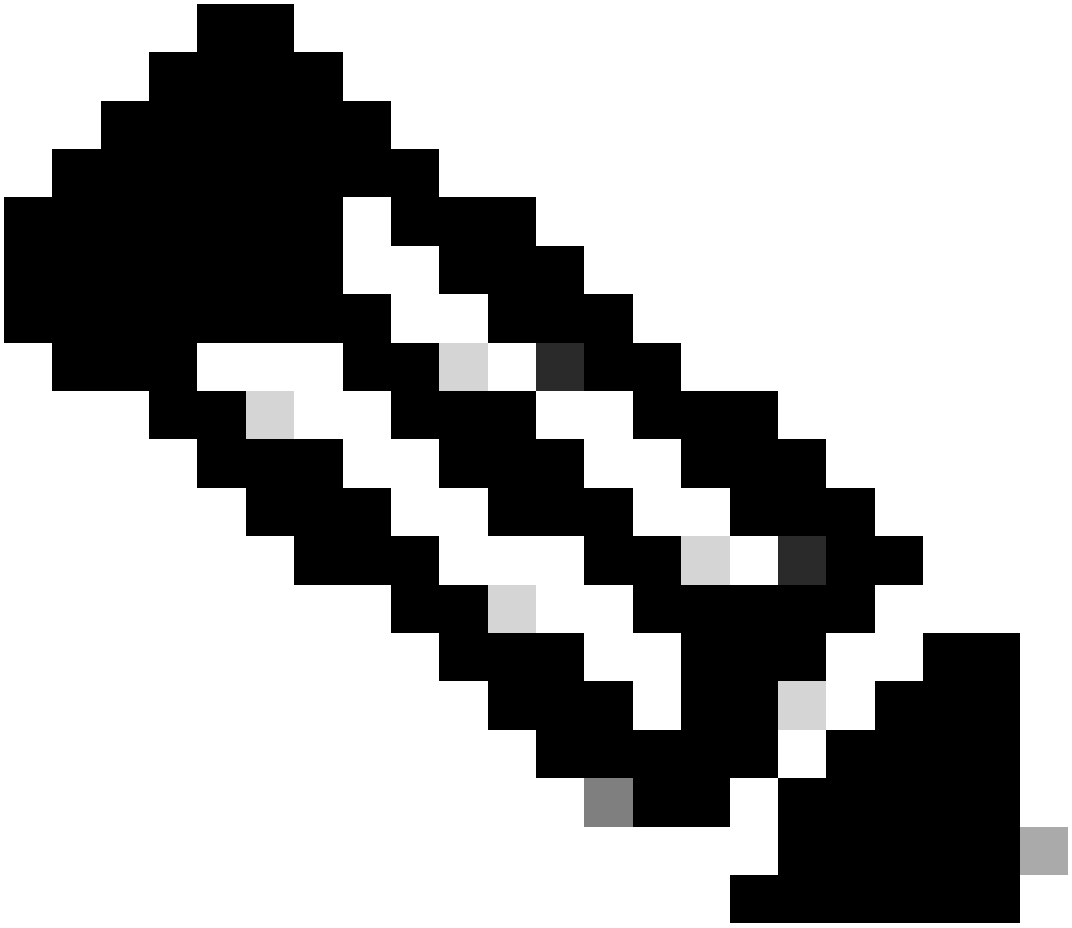
O QRadar da IBM é um SIEM popular para análise de registros. Ele fornece uma interface eficiente para analisar grandes blocos de dados, como os logs fornecidos pelo Cisco Umbrella para o tráfego DNS da sua organização. O Cisco Cloud Security App para IBM QRadar fornece informações de vários produtos de segurança (Investigar, Aplicar e CloudLock) e os integra ao QRadar. Ele também ajuda o usuário a automatizar a segurança e conter ameaças de forma mais rápida e direta do QRadar.

Quando você configura o aplicativo Cisco Cloud Security para QRadar, ele integra todos os dados da plataforma Cisco Cloud Security e permite que você visualize os dados em forma gráfica no console QRadar. No aplicativo, os analistas podem:

- Investigar domínios, endereços IP, endereços de e-mail
- Bloquear e desbloquear domínios (imposição)
- Exibir as informações de todos os incidentes da rede.

Este artigo descreve as instruções básicas para configurar e executar o QRadar para que ele possa extrair os logs do seu bucket S3 e consumi-los.

Requisitos



Note: O suporte para QRadar deve vir da IBM, pois a Cisco não pode oferecer suporte direto a hardware ou software de terceiros. Para quaisquer problemas de conexão do painel do Umbrella ao seu balde S3, podemos fornecer suporte. Muitas das informações encontradas aqui também podem ser encontradas no site da IBM: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umb

Requisitos do Cisco Umbrella

Este documento pressupõe que o bucket do Amazon AWS S3 foi configurado no Umbrella (Configurações > Gerenciamento de logs) e está mostrando verde com logs recentes que foram carregados.

Para obter mais informações sobre como configurar esse recurso, leia aqui: Manage Your Logs.

Requisitos do IBM Security Quad SIEM

O administrador deve ter direitos administrativos no(s) aparelho(s) QRadar, na configuração do

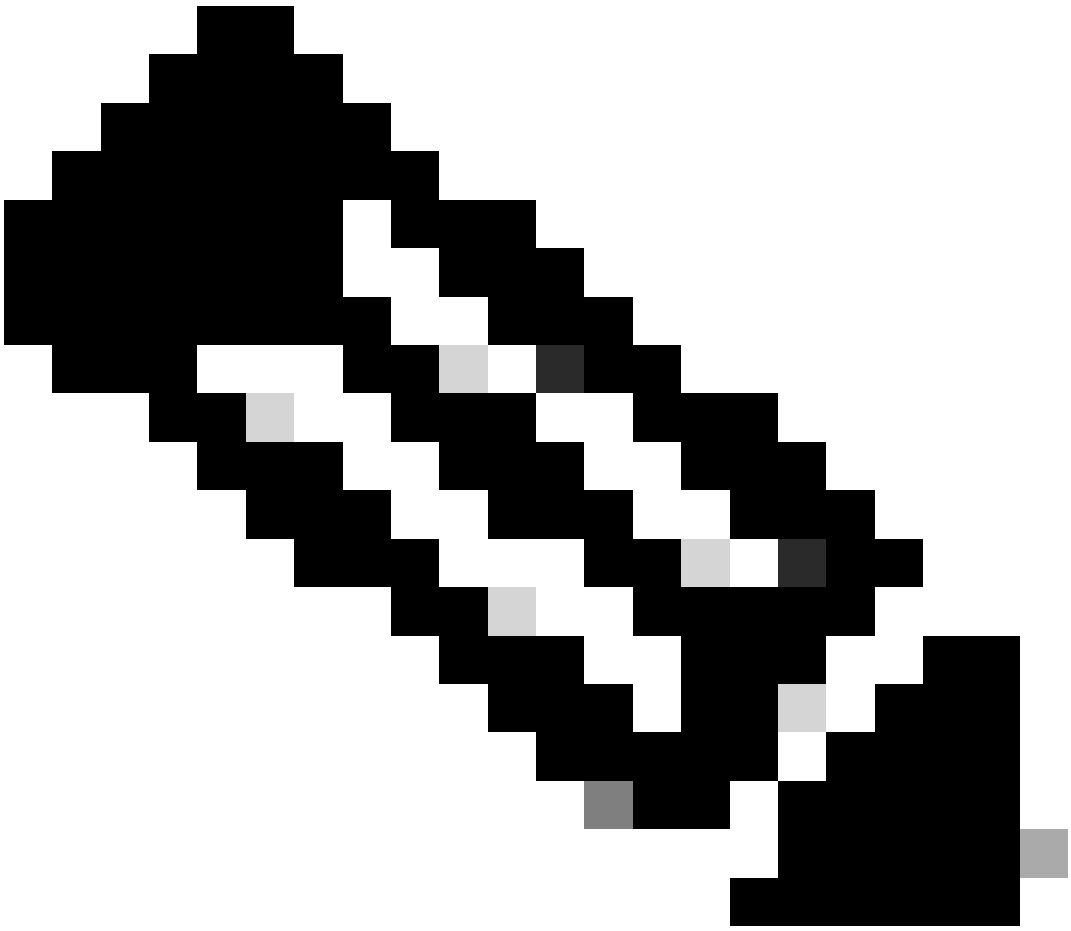
Amazon S3 e no painel Umbrella. Essas instruções supõem que o administrador do QRadar esteja familiarizado com a criação de arquivos LSX (extensão de origem de log).

Lembre-se de que o Cisco Cloud Security App v1.0.3 funciona somente até o IBM QRadar 7.2.8. A nova versão, v1.0.6, funciona com a versão QRadar atual de 7.4.2 e posterior.

Instalação do Cisco Cloud Security App para IBM QRadar

1. Faça o download e instale o Cisco Cloud Security App para IBM QRadar, que pode ser encontrado aqui: Cisco Cloud Security App v1.0.3 (para IBM QRadar v7.2.8) ou Cisco Cloud Security App v1.0.6 (para IBM QRadar v7.4.8).
2. Após a instalação, implante as alterações no QRadar.

Configuração do aplicativo Cisco Cloud Security: Adicionando fonte de log

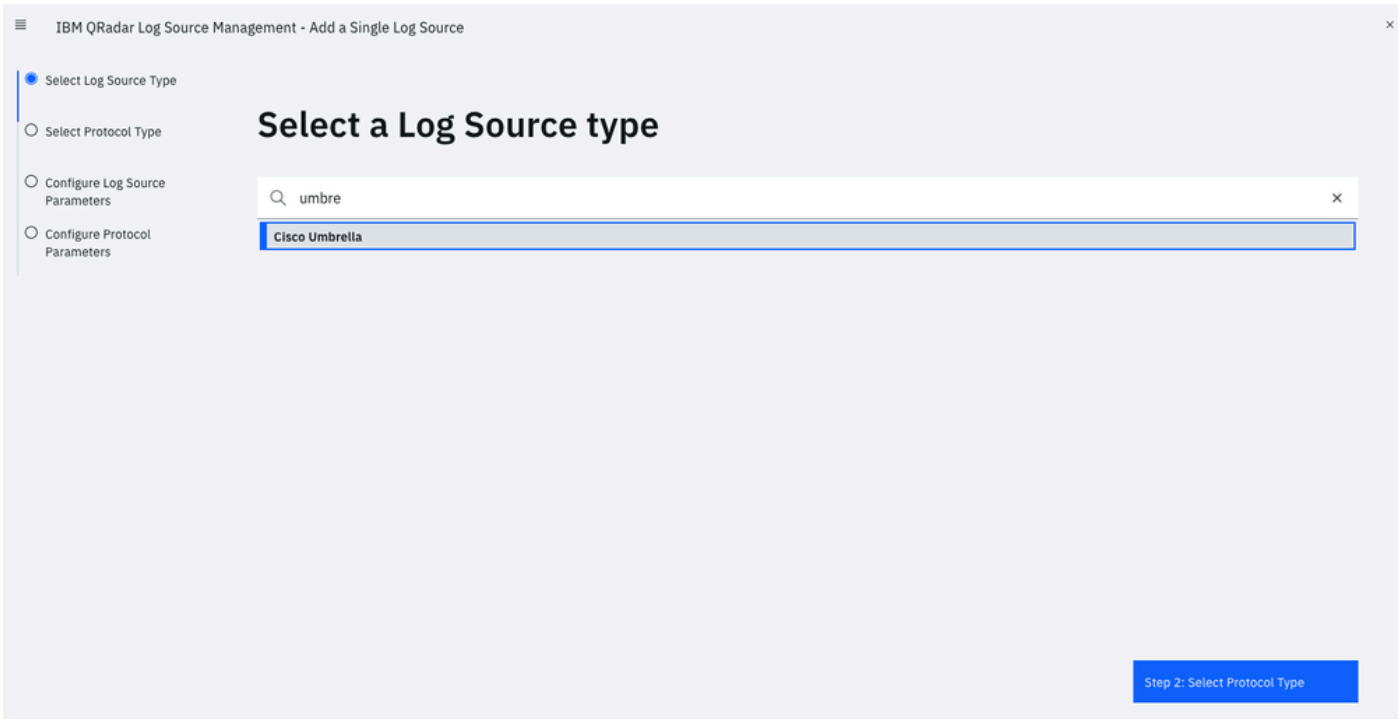


Note: Você pode ver outros registros em S3, como Auditoria e Firewall, mas eles não são suportados. Configure apenas os três listados aqui. Qualquer tentativa de configurar esses outros logs resulta em falha.

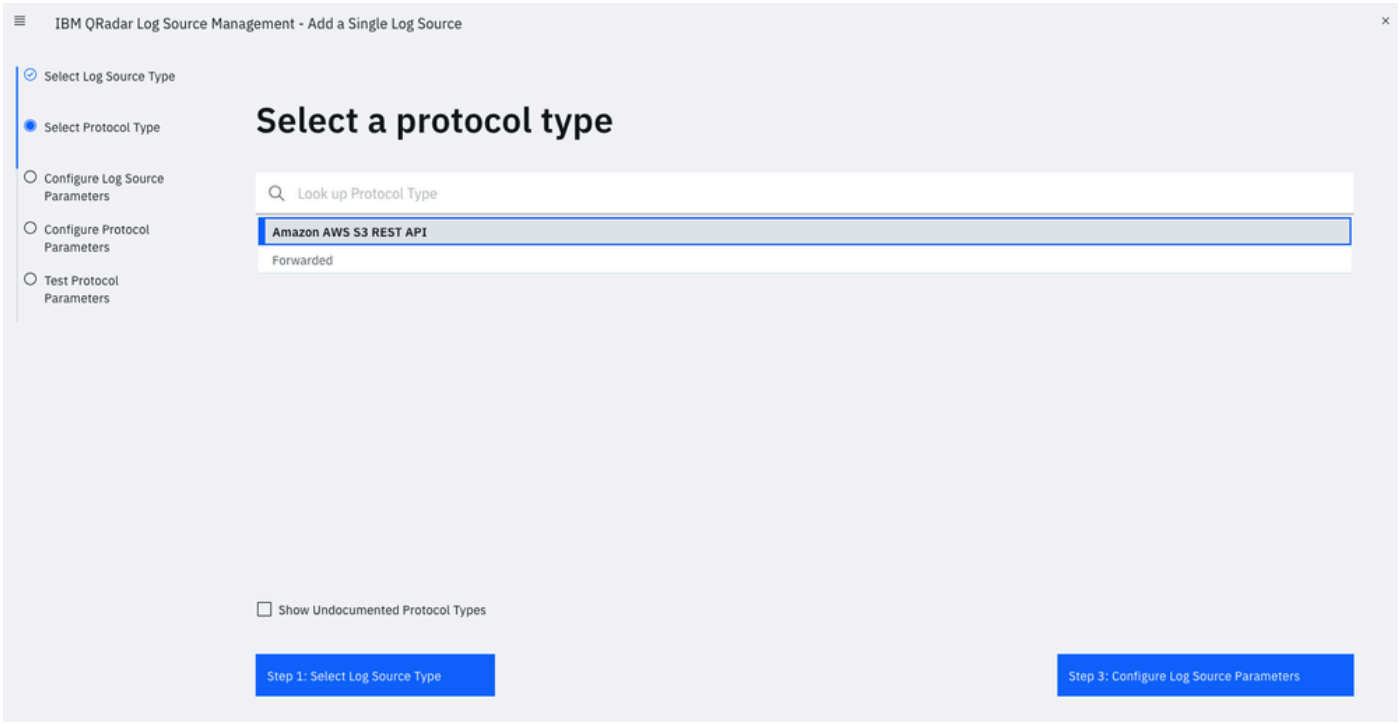
Para adicionar uma origem de log, clique na guia Admin na barra de navegação do QRadar, role para baixo e clique em QRadar Log Source Management, em seguida, clique no botão +New Log Source:

- Nome da origem do log (os nomes de entrada devem corresponder exatamente como listados):
  - Logs DNS da Cisco: cisco_umbrella_dns_logs
  - Logs IP do Cisco Umbrella: cisco_umbrella_ip_logs
  - Logs de proxy do Cisco Umbrella: cisco_umbrella_proxy_logs
- Formato do evento: CSV do Cisco Umbrella
- Tipo de Origem do Log: Guarda-chuva da Cisco
- Configuração de protocolo: API REST AWS S3 da Amazon
- Padrão do arquivo: .*?\.csv\.gz
- Extensão de Origem de Log: ** CiscoUmbrella_ext
- Selecione os grupos dos quais você deseja que esta origem de log seja membro: cisco_umbrella_logsource_group

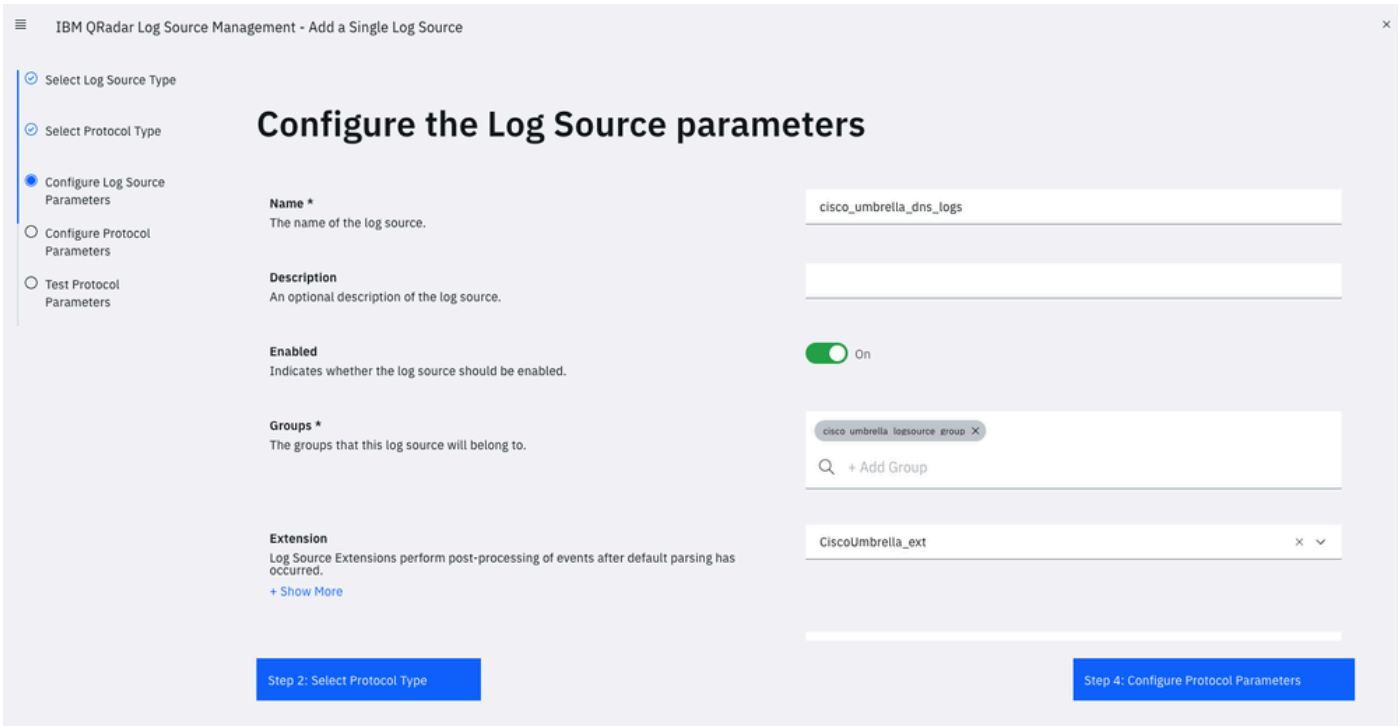
Vá para o Assistente para Adicionar uma única origem de log:



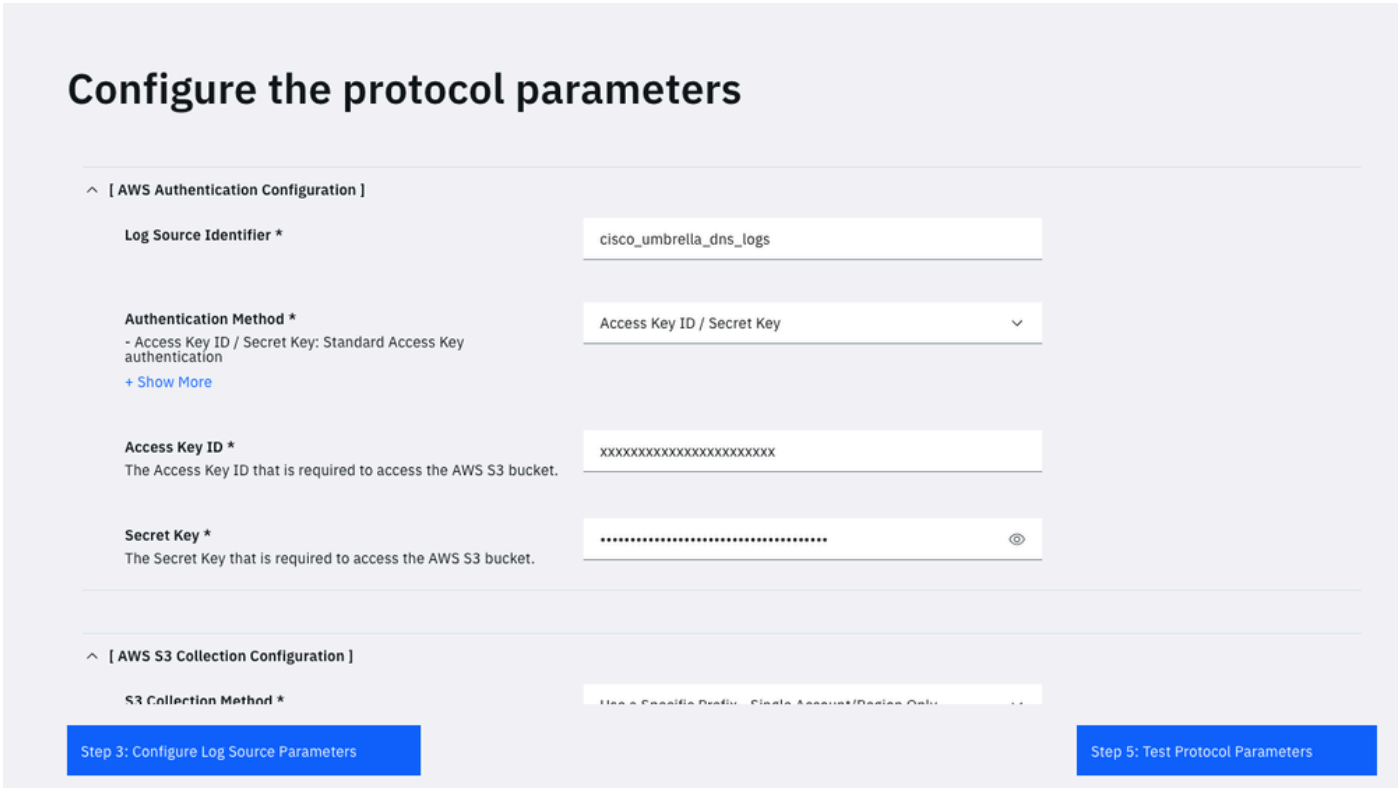
4404306773524



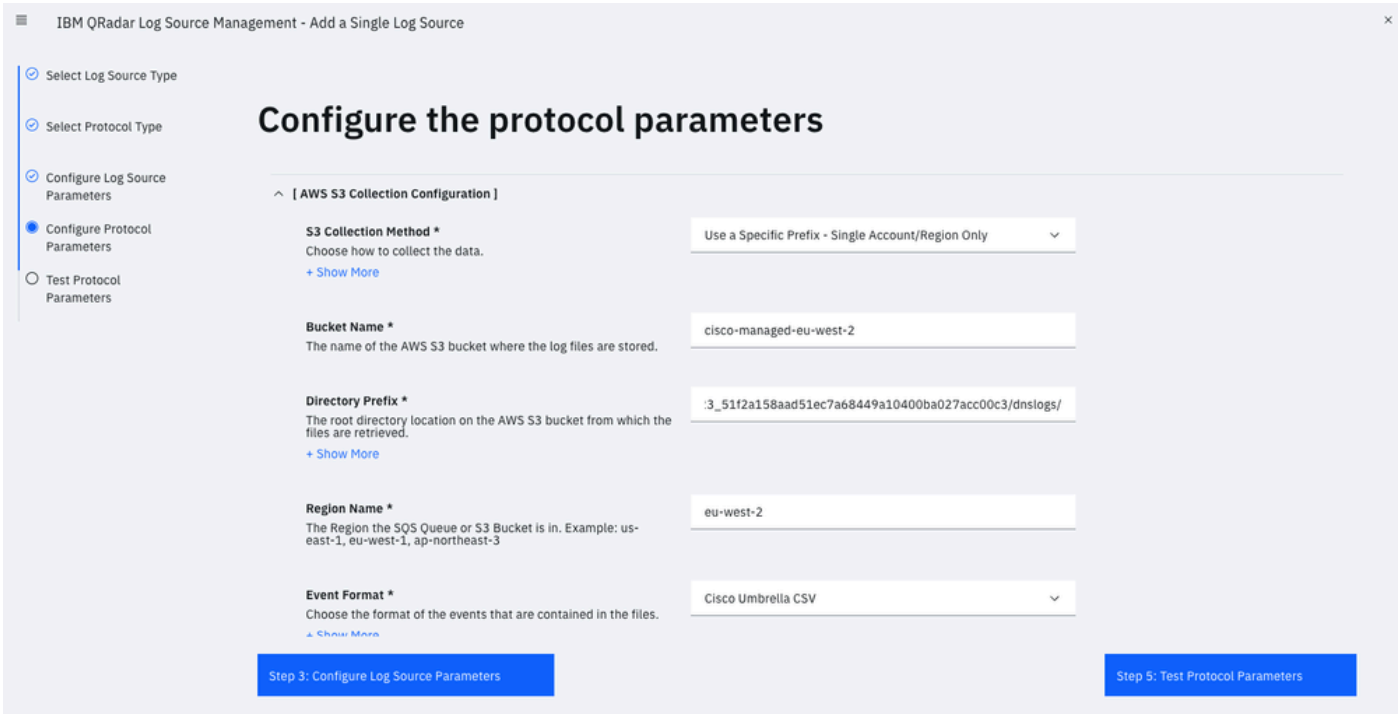
4404306773268



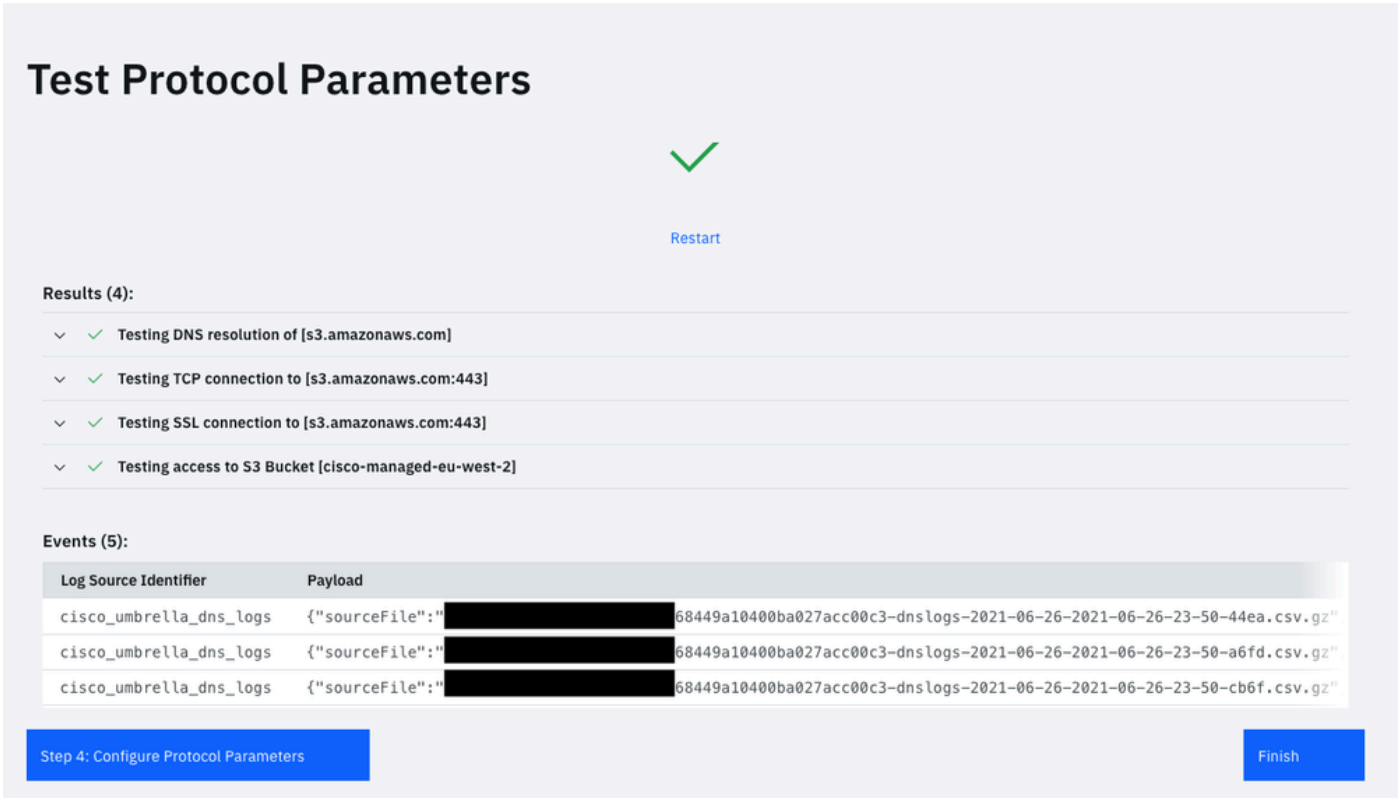
4404313505300



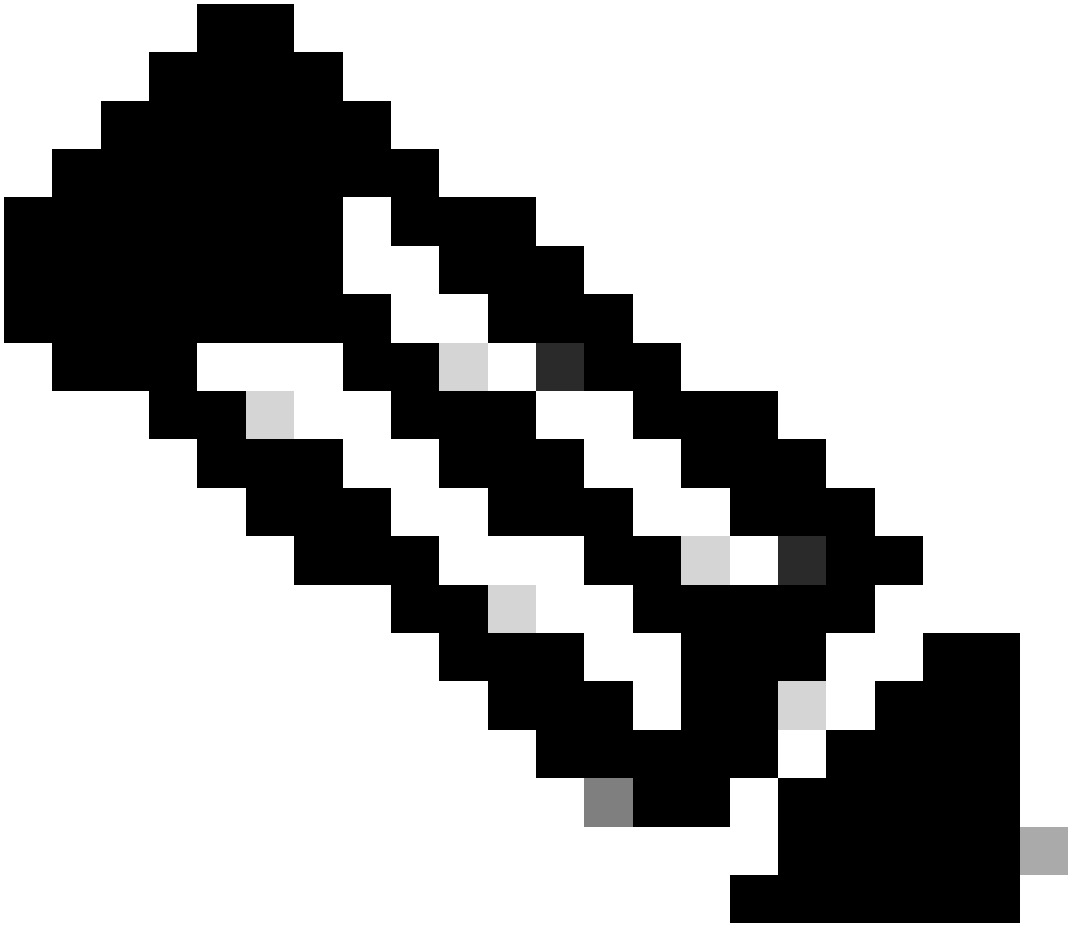
4404306774164



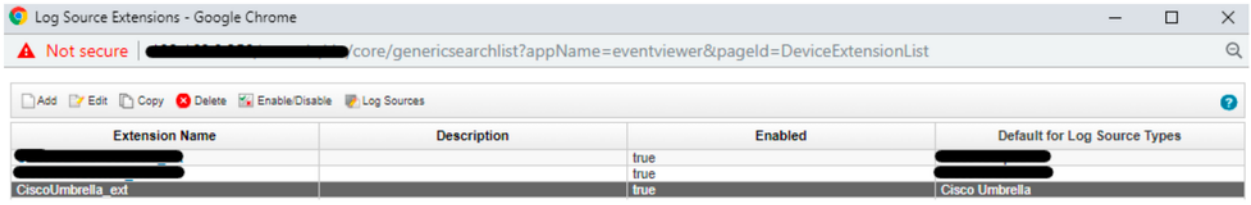
4404306897556



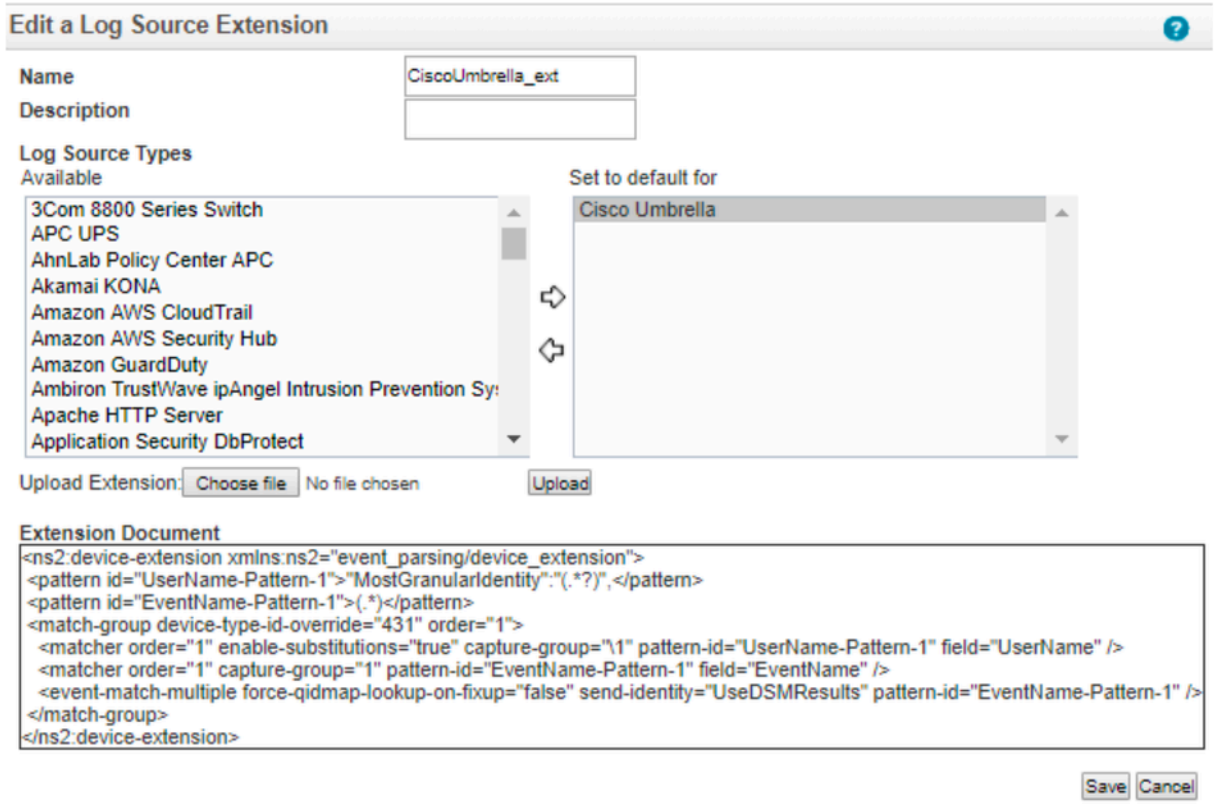
4404306881812



Note: Se a extensão da origem de log não estiver mapeada para "CiscoUmbrella_ext", escolha o nome da origem de log na lista:



360071157752



360071326791

Aqui está um exemplo de como é um Cisco Managed Bucket:

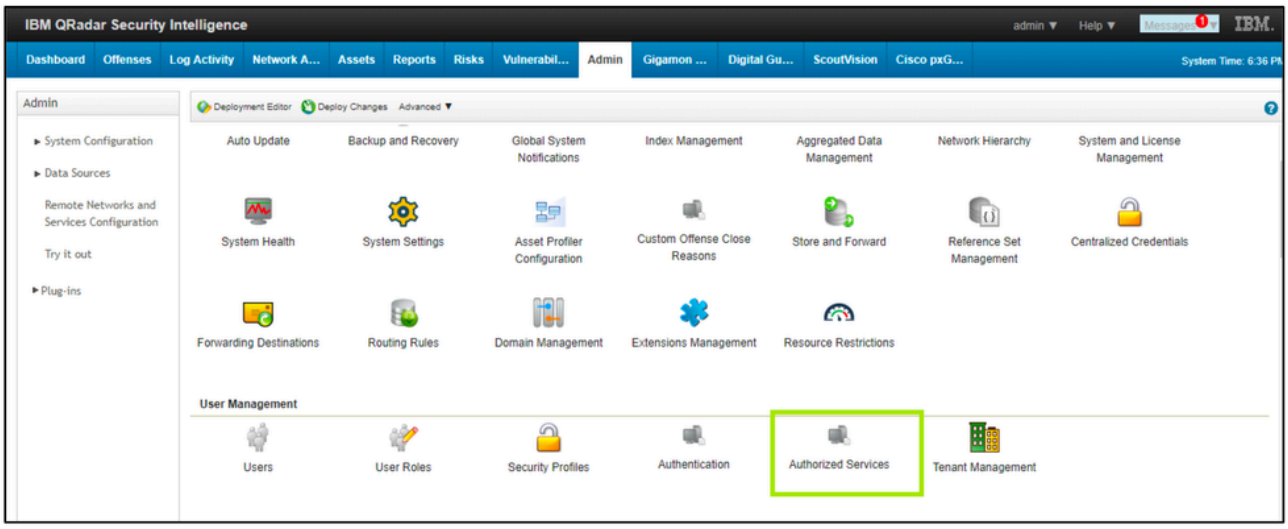
```
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxxx/dnslogs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

Navegue de volta para Cisco Cloud Security App Settings e defina a taxa de atualização do painel em horas com um valor mínimo de "1" para que os gráficos exibam dados.

Gerando token de autenticação

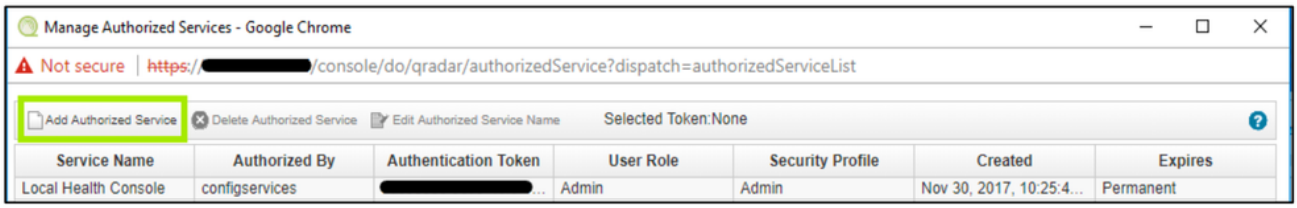
O administrador precisa gerar um token de serviço para adicionar ao seu aplicativo de segurança da Cisco. Como prática recomendada, o Token de serviço autorizado foi recriado a cada 90 dias:

1. Faça login no QRadar > guia Admin > Serviços autorizados.



360071965571

2. Adicionar serviços autorizados.

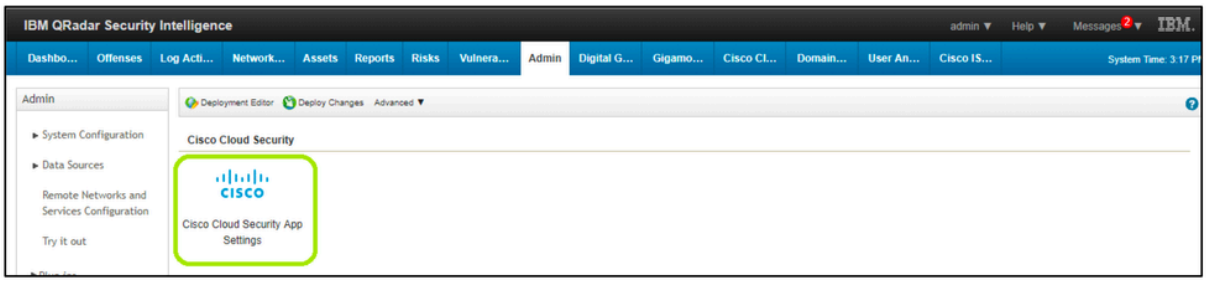


360071965551

3. Insira os detalhes e gere o token de autenticação.
4. Depois de gerar o token, clique em "Implantar alterações".

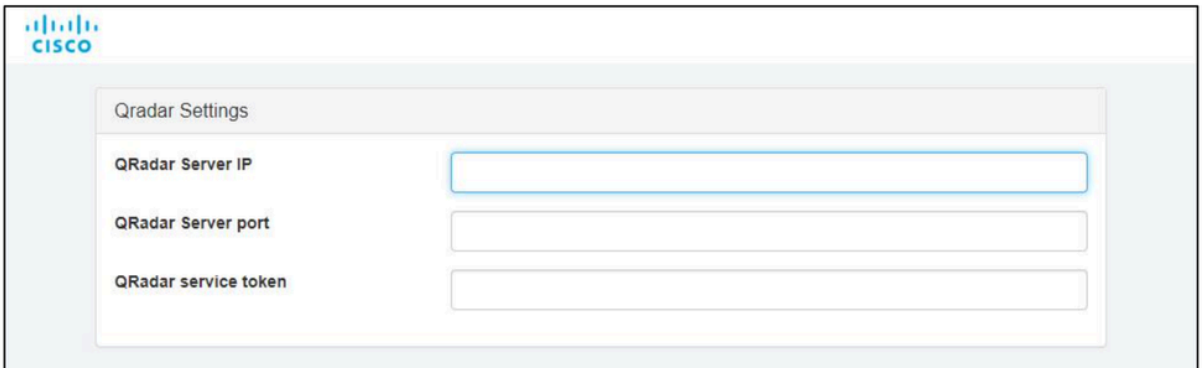
Configurando o aplicativo Cisco Cloud Security

1. Na guia Admin na barra de navegação do QRadar, role para baixo e abra Configurações do aplicativo Cisco Cloud Security.



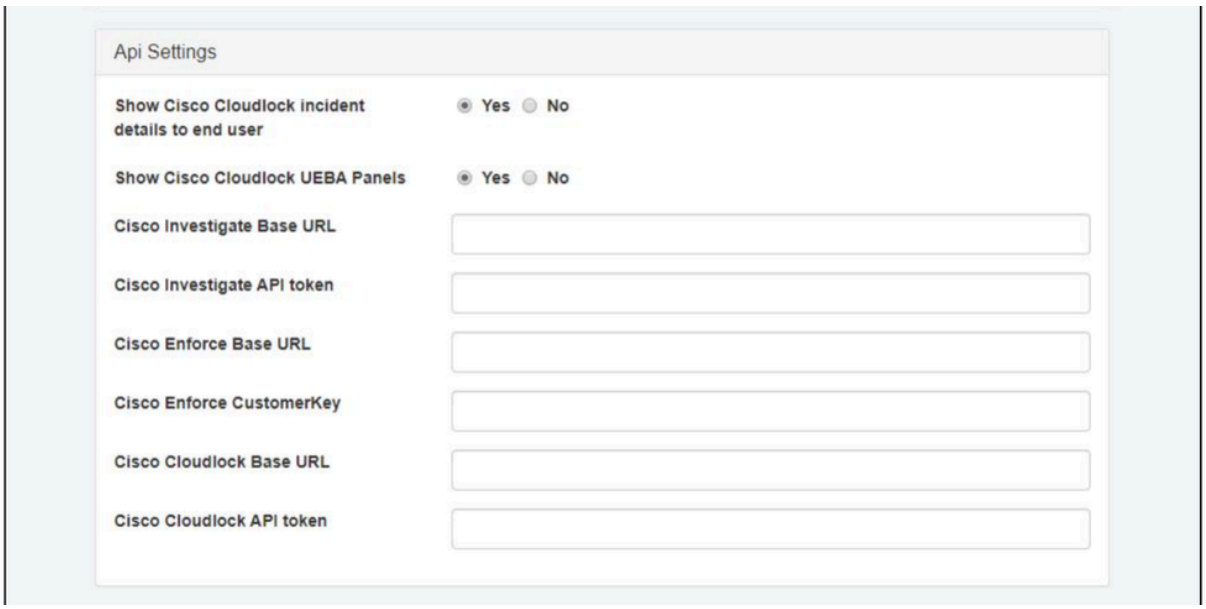
360071754732

2. Insira o token de autenticação gerado na etapa anterior.



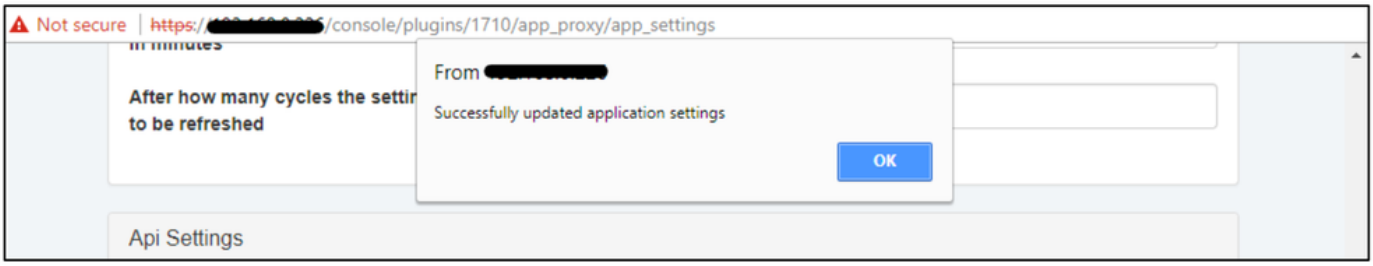
360072462992

3. Edite as Configurações da Api da seguinte maneira:
    - URL base de investigação da Cisco: https://investigate.api.umbrella.com/
    - Token de API de investigação da Cisco: gerar por meio do painel Umbrella -> Investigar -> Chaves API -> Criar novo token; para obter mais informações, consulte https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key
    - URL base de aplicação da Cisco: https://s-platform.api.opendns.com/1.0/
    - Cisco Enforce CustomerKey: gerar por meio do painel Umbrella -> Componentes de política -> Integrações -> Adicionar; para obter mais informações, consulte https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations
    - URL base do Cisco Cloudlock: https://{YourCloudlockAPIServer}/api/v2 (por exemplo, https://api-demo.cloudlock.com/api/v2/. Confirme a URL base do Cloudlock, também conhecida como URL da API do Cloudlock Enterprise, enviando um e-mail para support@cloudlock.com.)
    - Token de API do Cisco Cloudlock: gerar via Cloudlock -> Configurações -> Autenticação & API -> Gerar; para obter mais informações, consulte https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication



360072703611

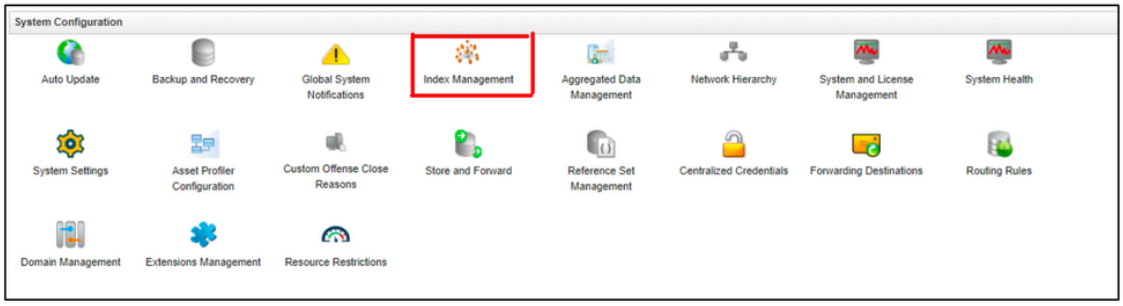
Um pop-up indica que as configurações do aplicativo foram atualizadas com êxito.



360071986151

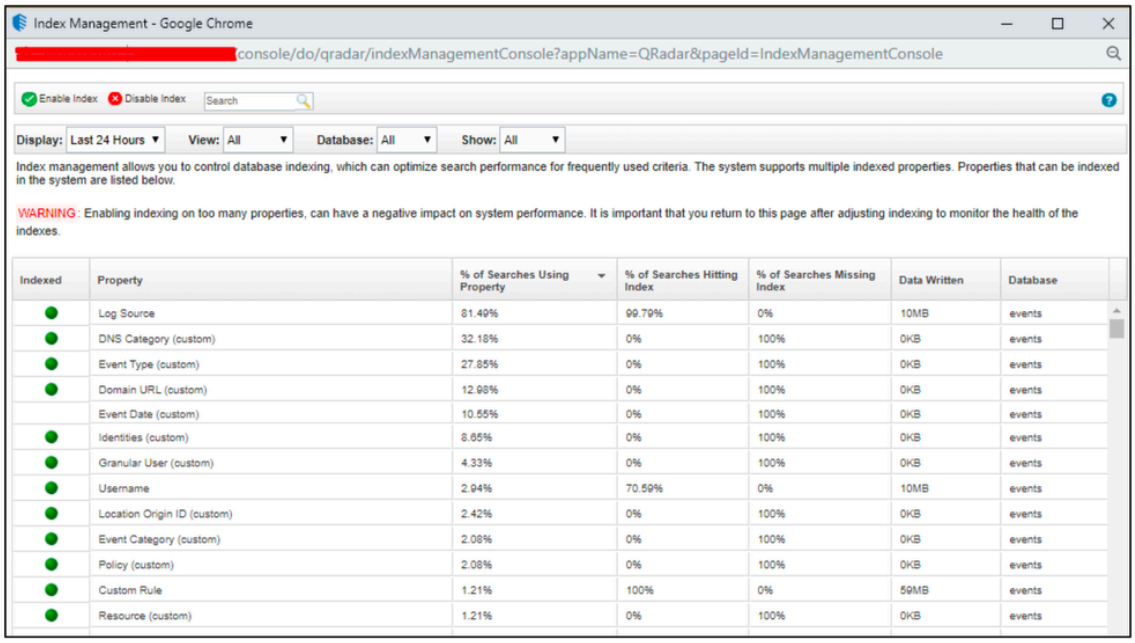
Indexação no QRadar

1. Navegue até a guia Admin e clique em Index Management.



360071780112

2. Indexe os CEPs Empacotados com o aplicativo.



360071988811

Estes são os CEPs recomendados a serem indexados:

1. Origem do log
2. Categoria DNS
3. Tipo de evento
4. URL do domínio
5. Identidades
6. Usuário granular
7. Nome de usuário
8. ID da Origem do Local
9. Categoria do evento
10. Política
11. Recurso

Agora você está pronto para usar o QRadar para iniciar as atividades de monitoramento dos detalhes do Cisco Umbrella, Investigate e CloudLock. Mais instruções sobre como navegar no QRadar podem ser encontradas aqui: Navegação no aplicativo Cisco Cloud Security.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.