为IBM QRadar配置云安全应用

目录

简介

本文档介绍如何使用IBM QRadar配置思科云安全应用以进行日志分析。

概述

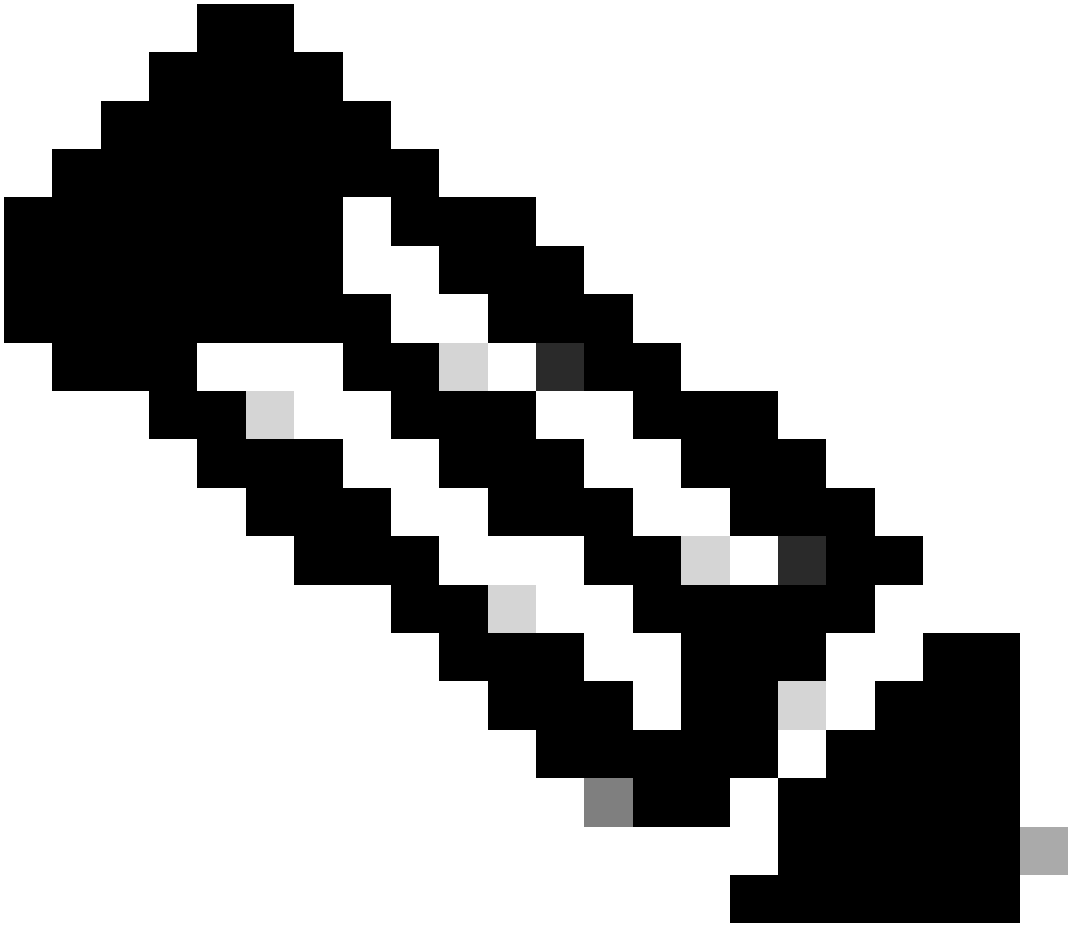
IBM的QRadar是常用的日志分析SIEM。它提供强大的接口来分析大数据块，例如Cisco Umbrella为您的组织的DNS流量提供的日志。适用于IBM QRadar的思科云安全应用提供多种安全产品（调查、实施和CloudLock）的洞察力，并将它们与QRadar集成。它还可以帮助用户从QRadar中更快且直接地自动执行安全并遏制威胁。

当您为QRadar设置思科云安全应用时，它集成了思科云安全平台的所有数据，并允许您在QRadar控制台中以图形形式查看数据。从应用中，分析师可以：

- 调查域、IP地址、邮件地址
- 阻止和取消阻止域（实施）
- 查看网络所有事件的信息。

这篇文章概述了设置QRadar并运行QRadar的基本方法，以便从S3存储桶中提取日志并使用日志。

要求



注意：对QRadar的支持必须来自IBM，因为思科无法直接支持第三方硬件或软件。对于将您的Umbrella控制面板连接到S3存储桶的任何问题，我们可以提供支持。IBM网站上也有许多此处提供的信息
：https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Ur

Cisco Umbrella要求

本文档假设您的Amazon AWS S3存储桶已在Umbrella（设置>日志管理）中配置，并且显示绿色，并且已上传最近的日志。

有关如何配置此功能的详细信息，请阅读此处：管理日志。

IBM Security QRadar SIEM要求

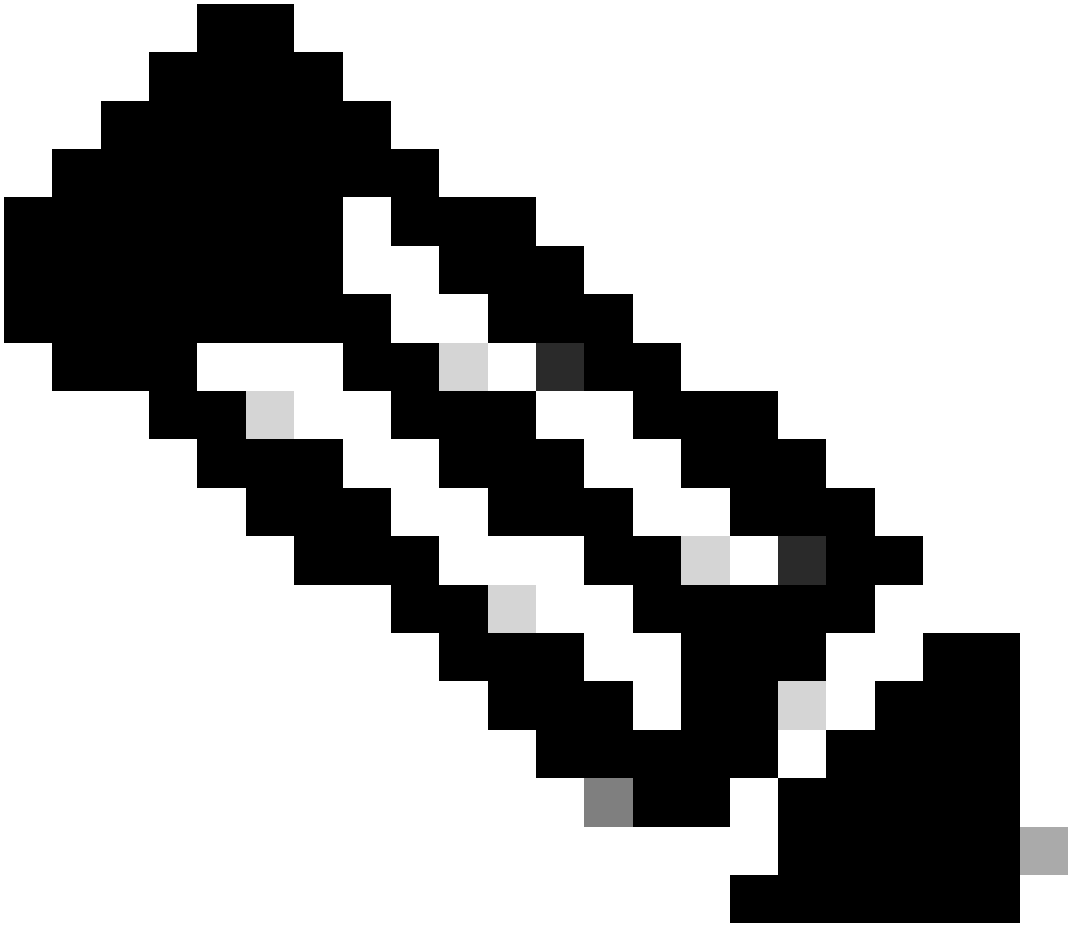
管理员需要拥有QRadar设备、Amazon S3配置和Umbrella控制面板的管理权限，这些说明假设QRadar管理员熟悉创建LSX(Log source Extension)文件。

请注意，思科云安全应用v1.0.3仅适用于IBM QRadar 7.2.8。新版本v1.0.6适用于当前7.4.2及更高版本的QRadar。

安装适用于IBM QRadar的思科云安全应用

1. 下载并安装适用于IBM QRadar的思科云安全应用，网址为：Cisco Cloud Security App v1.0.3(适用于IBM QRadar v7.2.8)或Cisco Cloud Security App v1.0.6（适用于IBM QRadar v7.4.8）。
2. 安装后，在QRadar中部署更改。

思科云安全应用配置：添加日志源



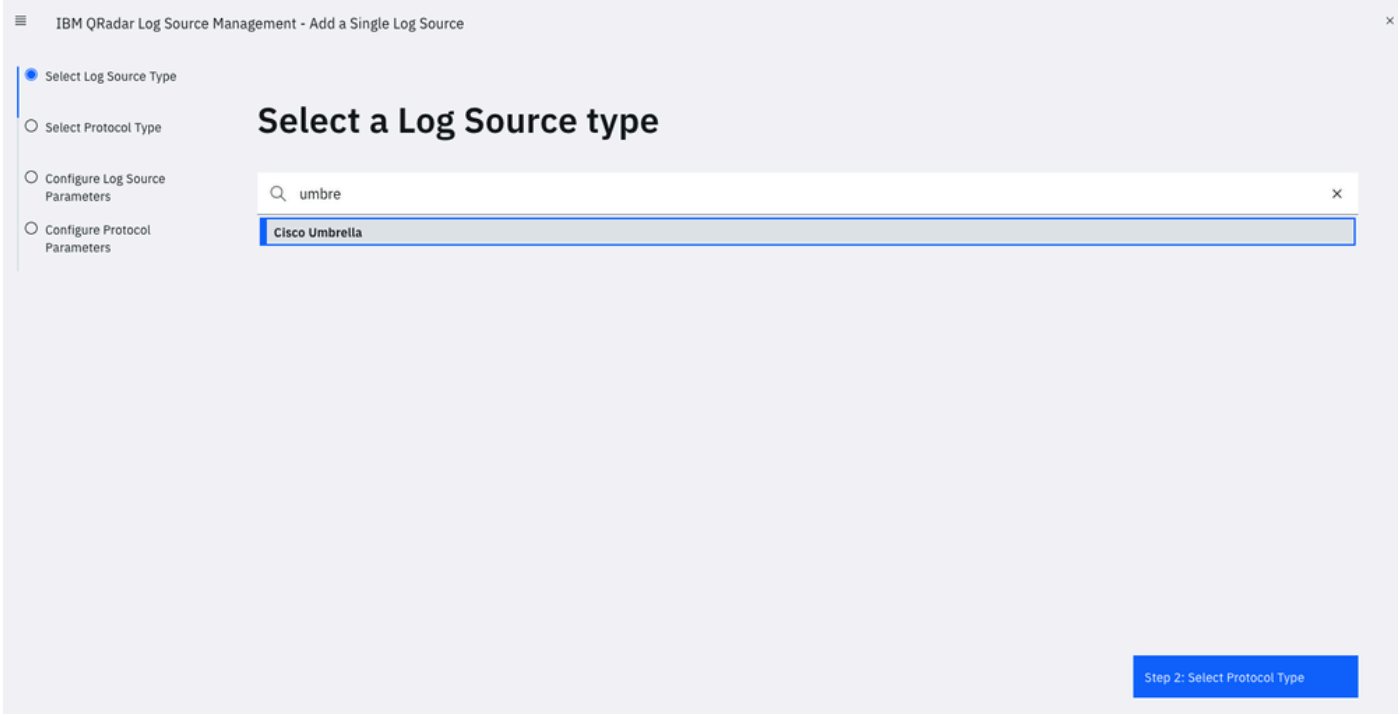
注意：您可以在S3中看到其他日志，例如审计和防火墙，但不支持这些日志。只设置此处列出的三个选项。任何配置其他日志的尝试都会导致失败。

要添加日志源，请点击QRadar导航栏上的Admin选项卡，向下滚动并点击QRadar Log Source

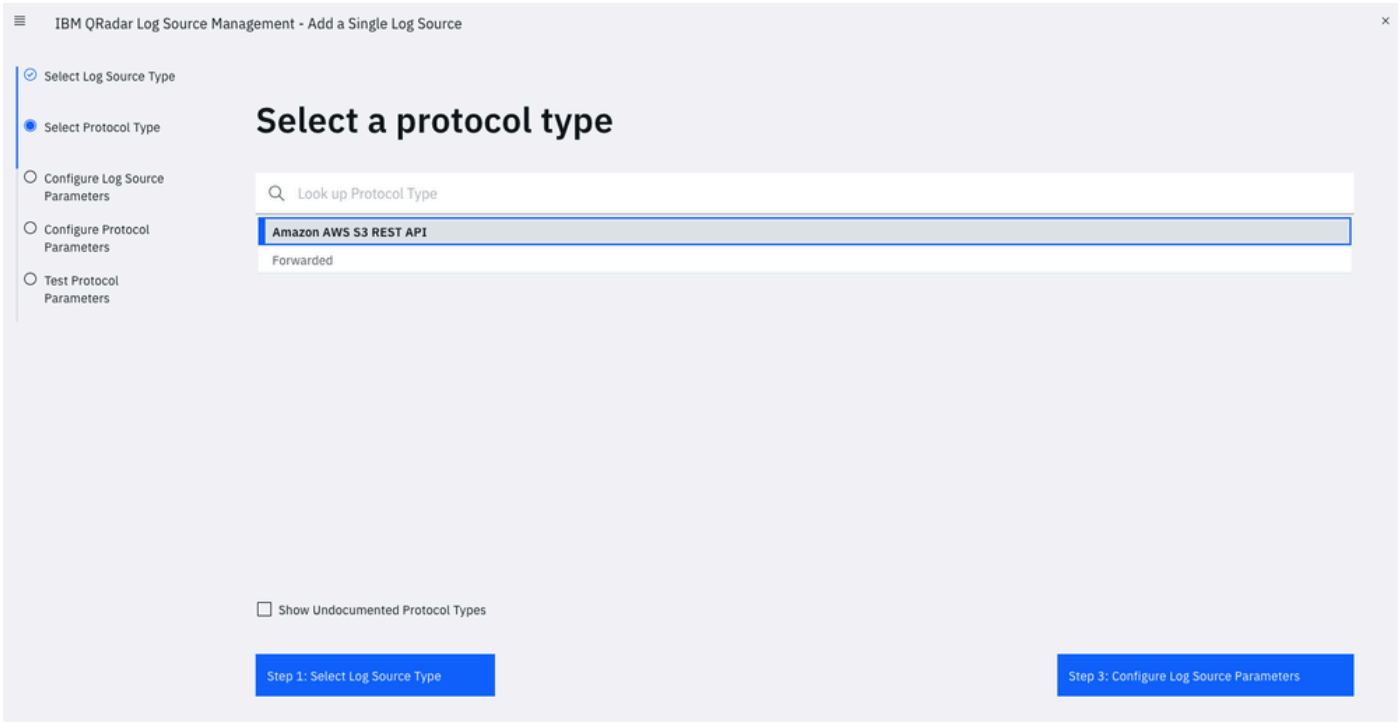
Management，然后点击按钮+New Log Source:

- 日志源名称（条目名称必须完全与列出的名称匹配）：
  - 思科DNS日志：cisco_umbrella_dns_logs
  - Cisco Umbrella IP日志：cisco_umbrella_ip_logs
  - Cisco Umbrella代理日志：cisco_umbrella_proxy_logs
- 事件格式：思科Umbrella CSV
- 日志源类型：思科雨伞
- 协议配置:Amazon AWS S3 REST API
- 文件模式：.*?\.csv\.gz
- 日志源扩展：CiscoUmbrella_ext **
- 请选择您希望此日志源成为其成员的任何组：cisco_umbrella_logsource_group

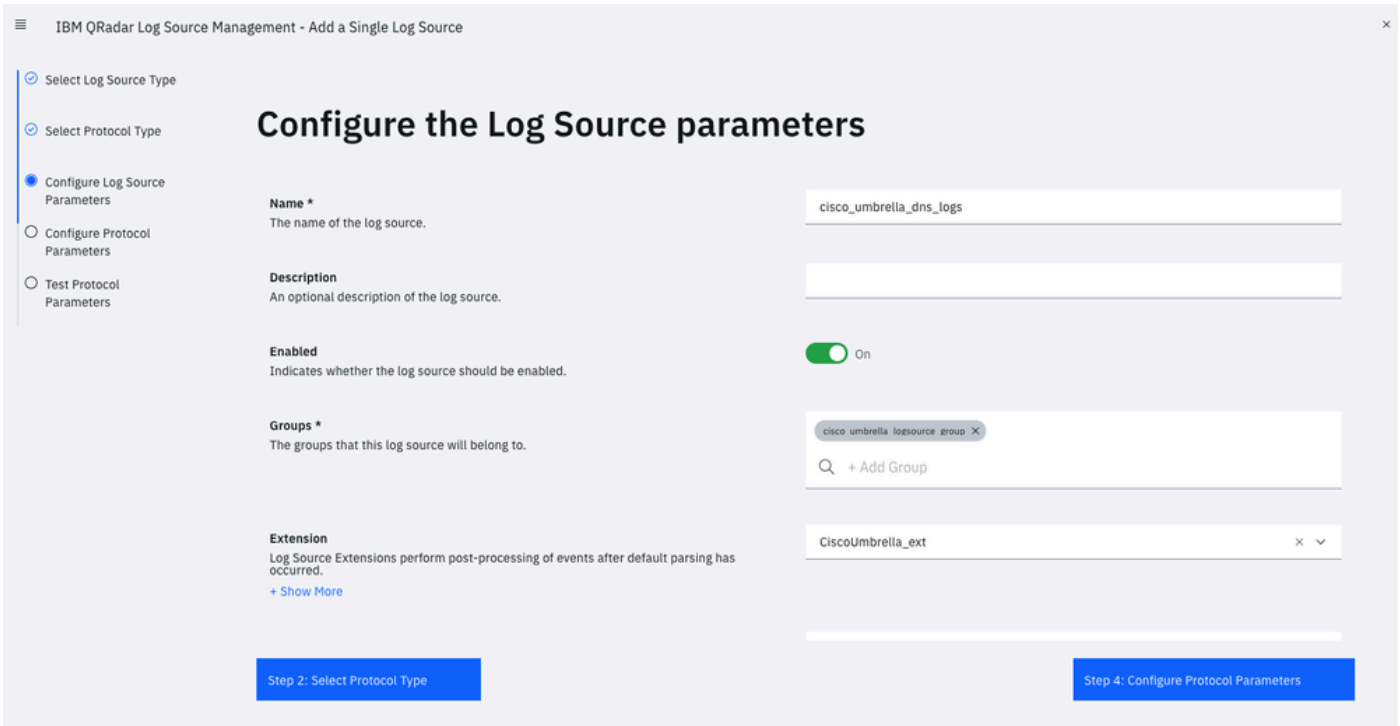
通过Add a Single Log Source向导：



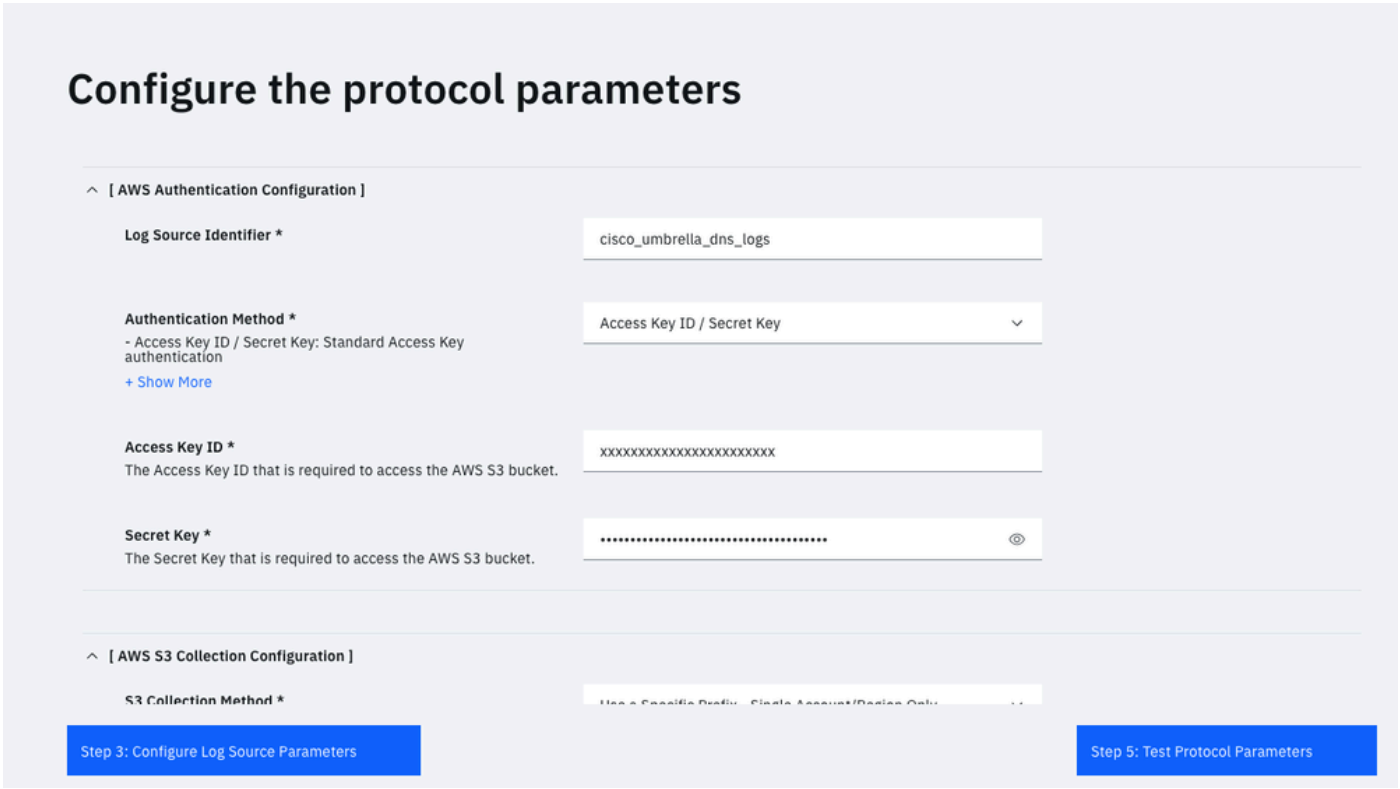
4404306773524



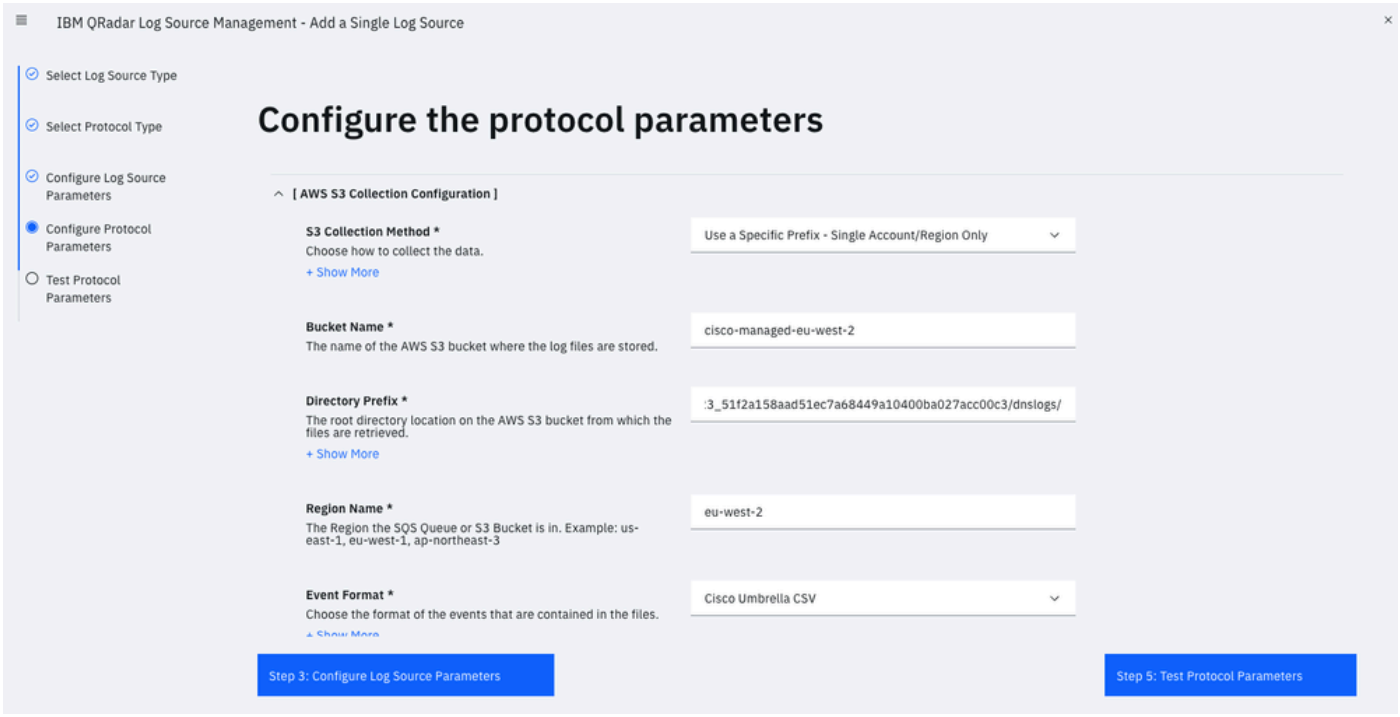
4404306773268



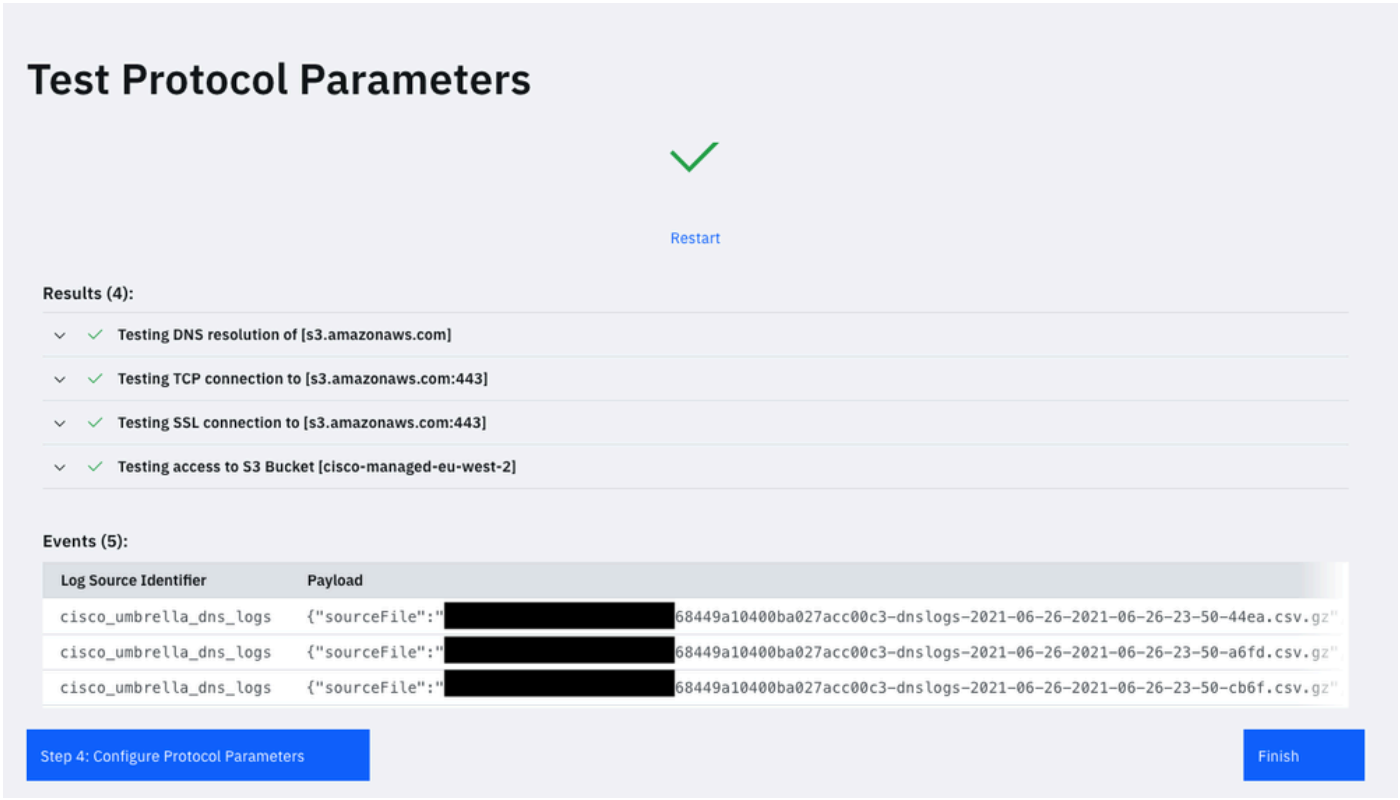
4404313505300



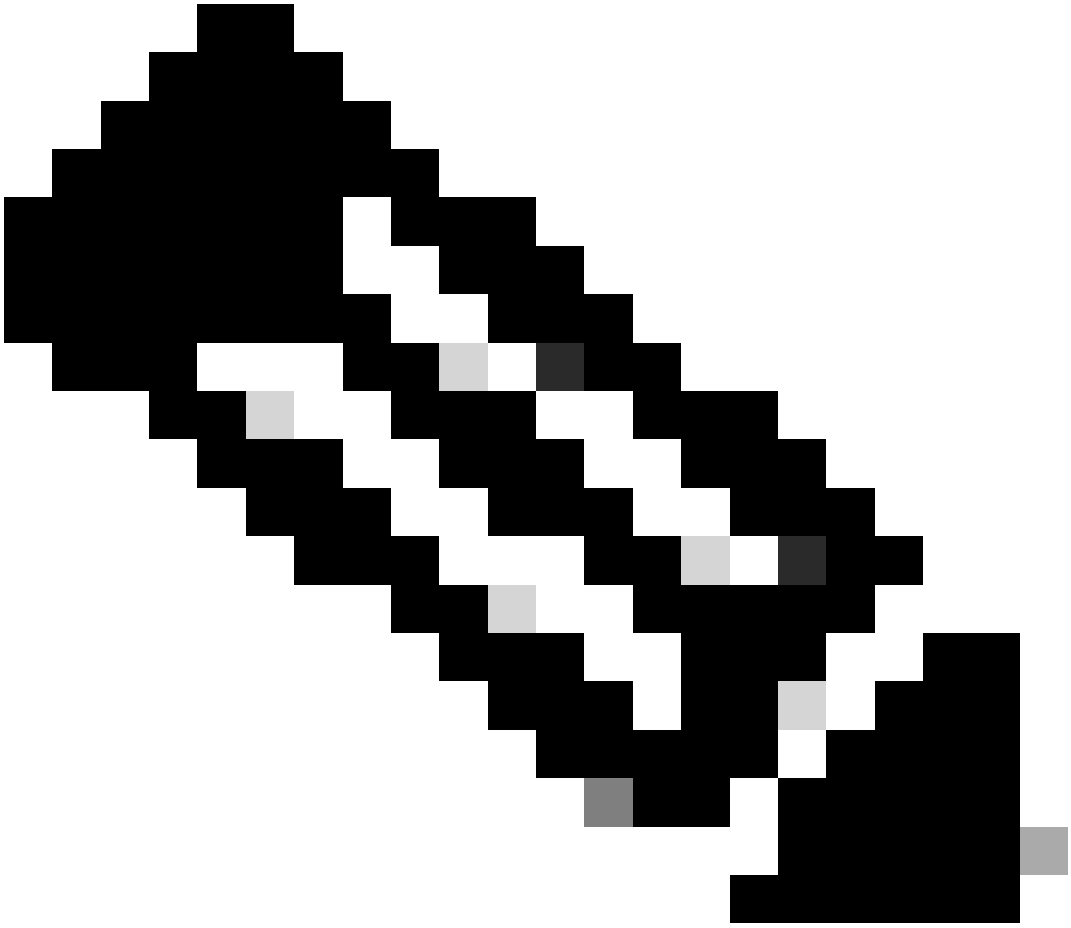
4404306774164



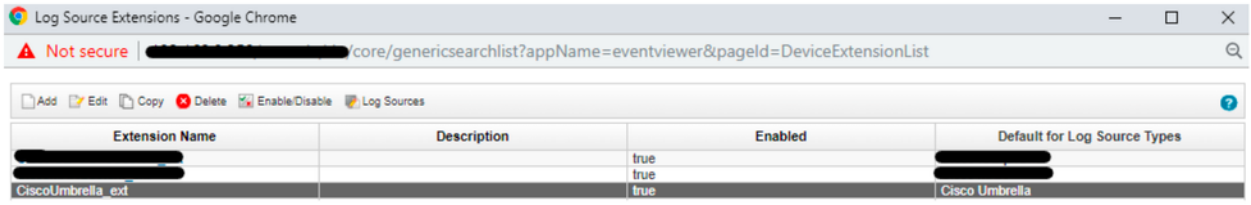
4404306897556



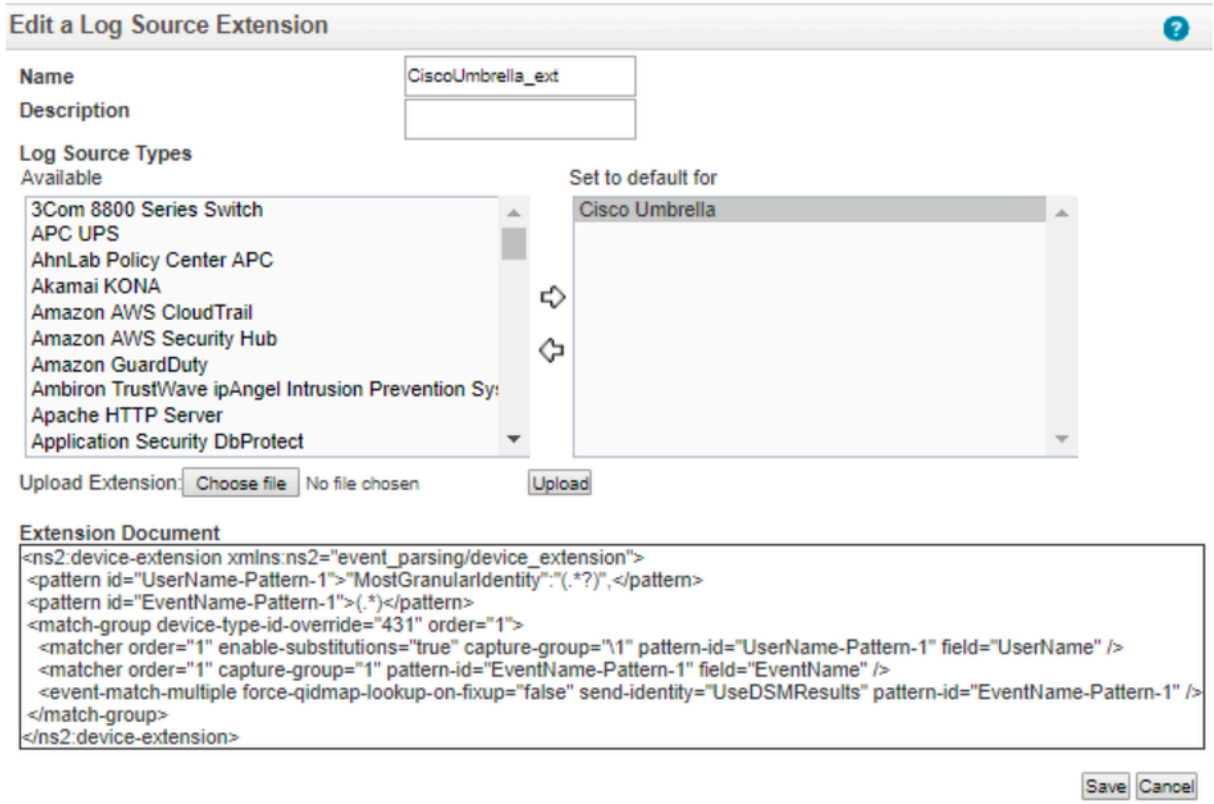
4404306881812



注意：如果日志源扩展未映射到“CiscoUmbrella_ext”，请从列表中选择日志源名称：



360071157752



360071326791

以下是Cisco Managed Bucket的示例：

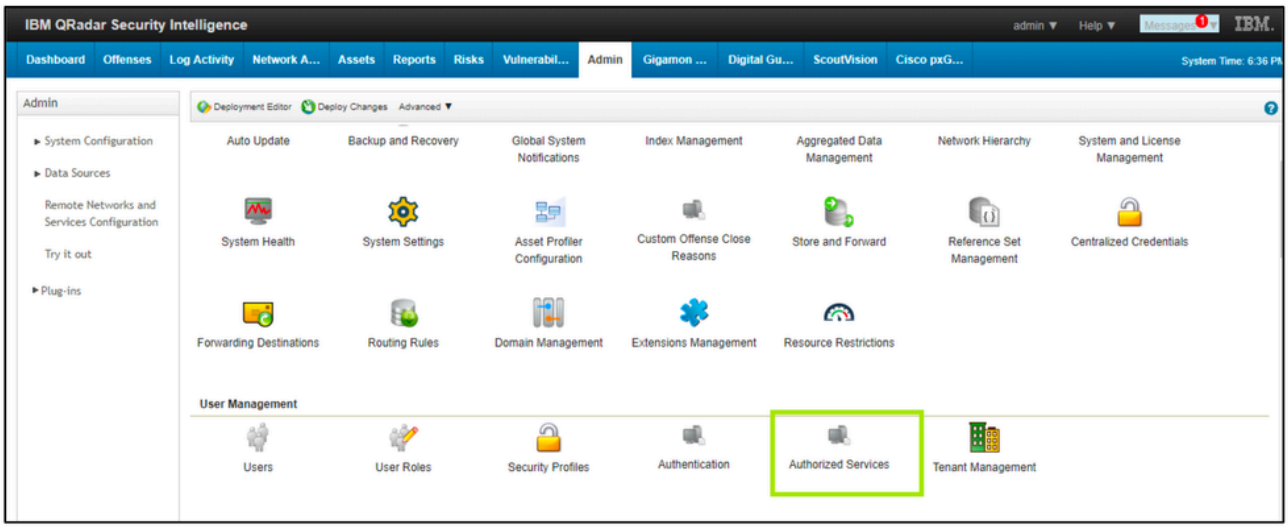
```
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxxx/dnslogs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

导航回Cisco Cloud Security App Settings，并将Panel refresh rate（以小时为单位）设置为最小值“1”，以便图形显示数据。

生成身份验证令牌

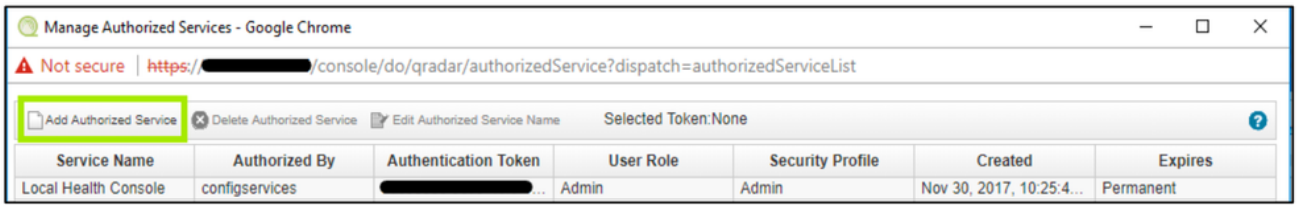
管理员需要生成服务令牌以添加到您的思科安全应用。作为最佳实践，每90天重新创建一次授权服务令牌：

1. 登录QRadar > Admin Tab > Authorized Services。



360071965571

2. 添加授权服务。

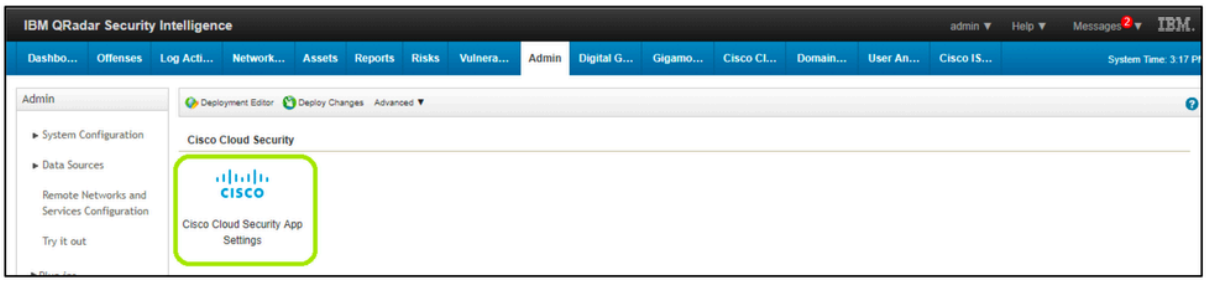


360071965551

3. 输入详细信息并生成身份验证令牌。
4. 生成令牌后，点击“部署更改”。

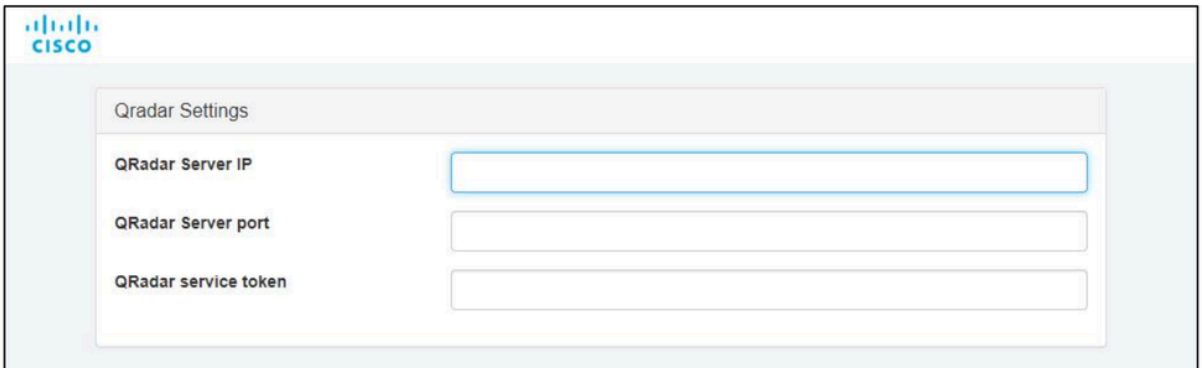
配置思科云安全应用

1. 从QRadar导航栏上的Admin选项卡，向下滚动并打开Cisco Cloud Security App Settings。



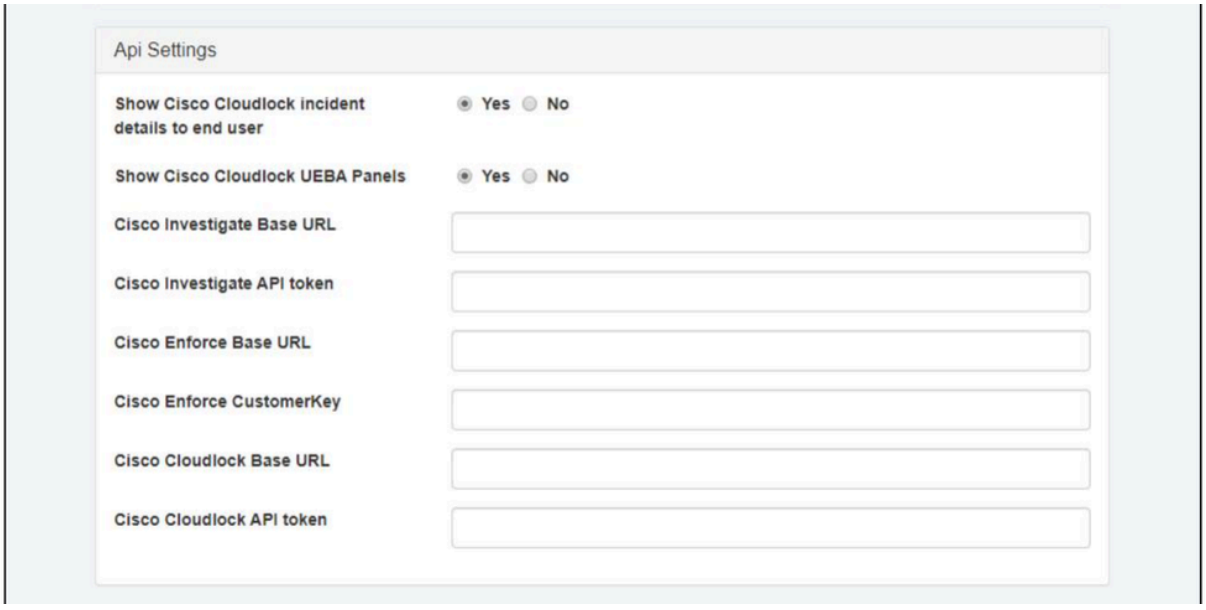
360071754732

2. 输入上一步中生成的身份验证令牌。



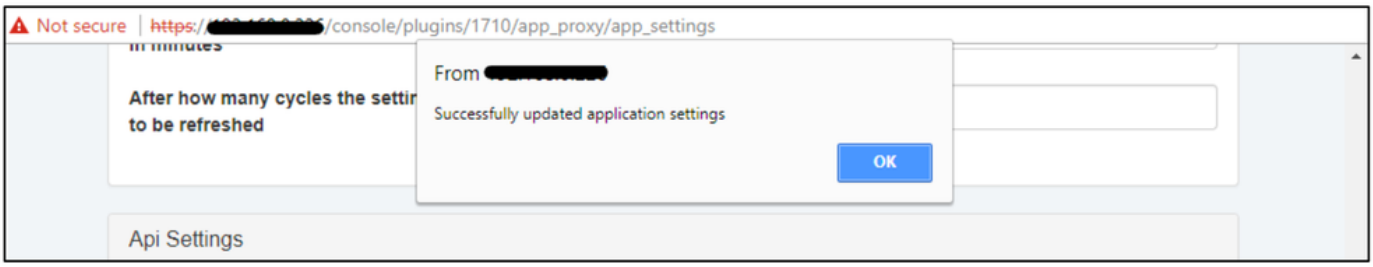
360072462992

3. 按如下方式编辑Api设置：
   - 思科调查基本URL:https://investigate.api.umbrella.com/
   - 思科调查API令牌： 通过Umbrella控制面板 — > Investigate -> API Keys -> Create New Token;有关详细信息，请参阅https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key
   - 思科实施基本URL:https://s-platform.api.opendns.com/1.0/
   - Cisco Enforce CustomerKey: 通过Umbrella控制面板 — > Policy Components -> Integrations -> Add;有关详细信息，请参阅https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations
   - Cisco Cloudlock基础URL:https://{YourCloudlockAPIServer}/api/v2(例如，https://api-demo.cloudlock.com/api/v2/。请通过向support@cloudlock.com发送电子邮件来确认您的Cloudlock Base URL，也称为Cloudlock Enterprise API URL。)
   - Cisco Cloudlock API令牌：通过Cloudlock -> Settings -> Authentication & API -> Generate;有关详细信息，请参阅https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication



360072703611

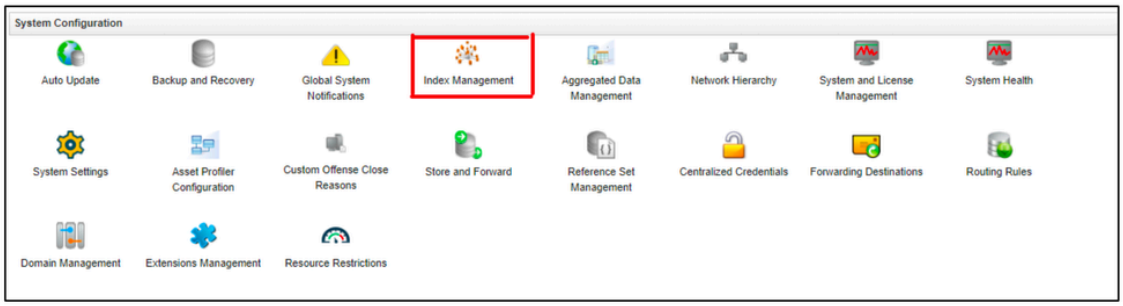
弹出窗口表示应用设置已成功更新。



360071986151

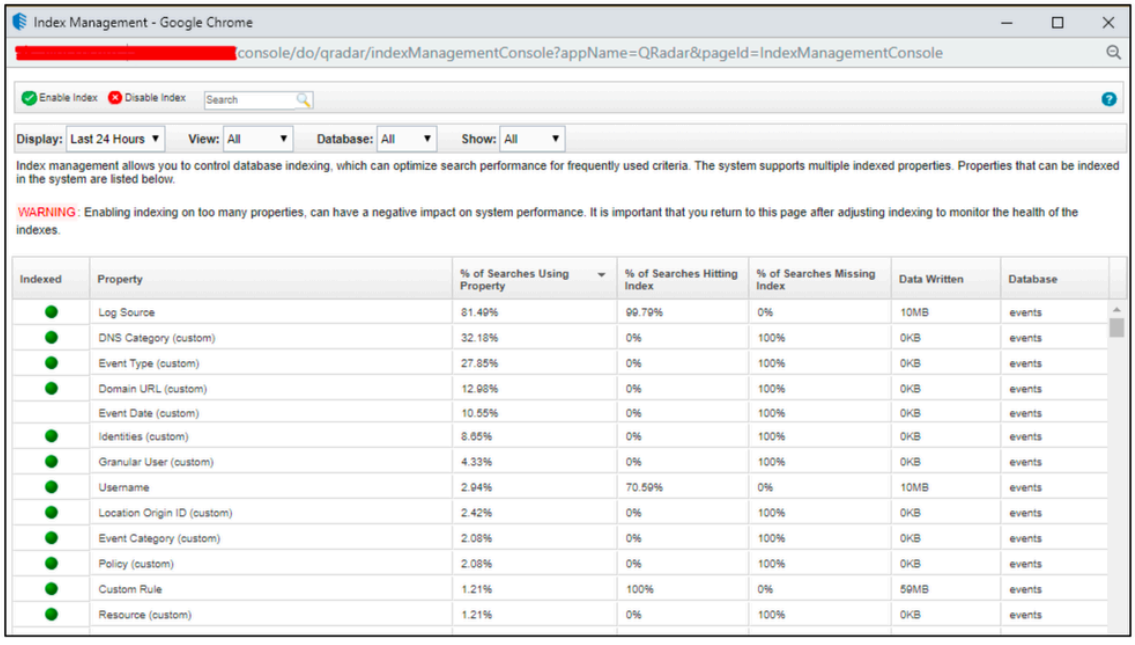
QRadar中的索引

1. 导航到Admin选项卡，然后单击Index Management。



360071780112

2. 为应用打包的CEP编制索引。



360071988811

以下是需要编制索引的建议CEP:

1. 日志源
2. DNS类别

3. 事件类型
4. 域URL
5. 身份
6. 精细用户
7. 用户名
8. 位置来源ID
9. 事件类别
10. 策略
11. 资源

现在，您已准备好使用QRadar开始监控Cisco Umbrella、Investigate和CloudLock详细信息的活动。有关如何导航QRadar的更多说明，请点击此处：导航思科云安全应用。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。