Konfigurieren der Cloud Security App für IBM QRadar

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die Cisco Cloud Security-Anwendung mit IBM QRadar für die Protokollanalyse konfiguriert wird.

Überblick

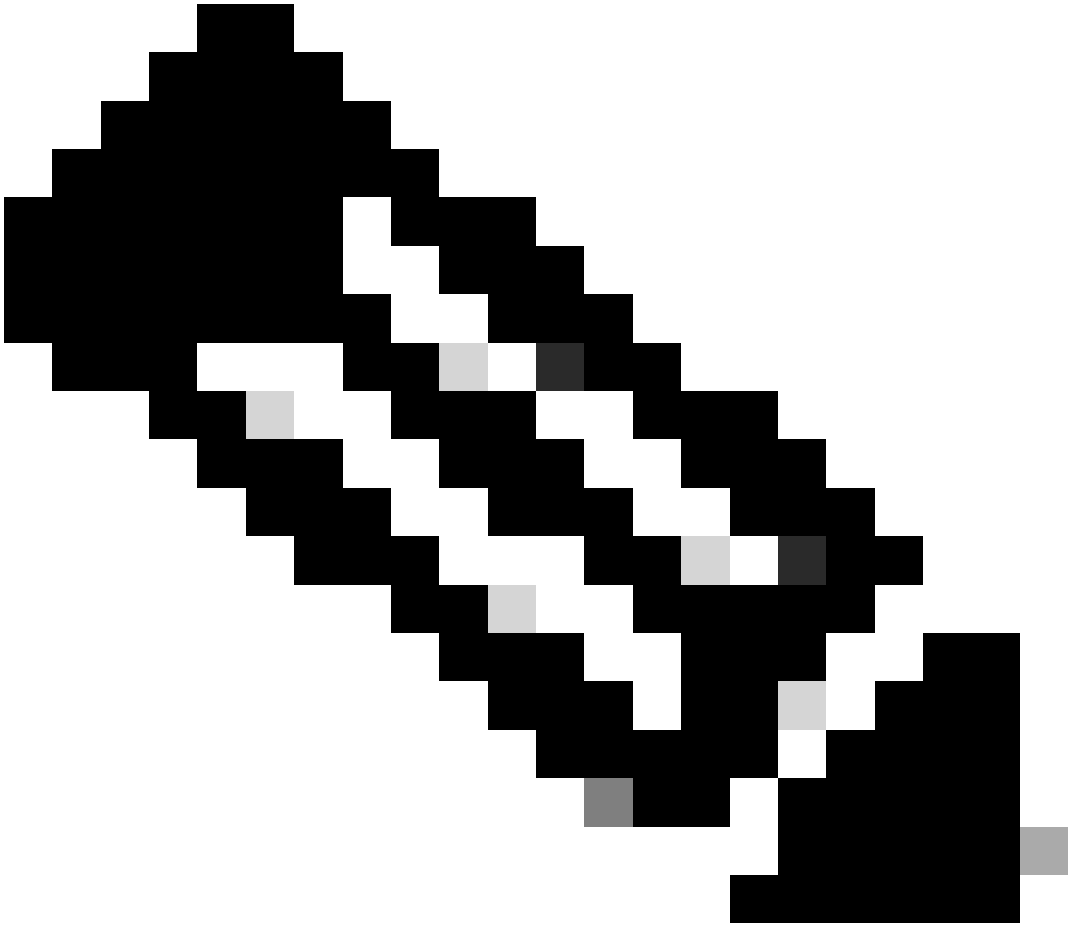
QRadar von IBM ist ein beliebtes SIEM für die Protokollanalyse. Es bietet eine leistungsstarke Schnittstelle für die Analyse großer Datenmengen, wie z. B. die von Cisco Umbrella bereitgestellten Protokolle für den DNS-Datenverkehr Ihres Unternehmens. Die Cisco Cloud Security App für IBM QRadar bietet Einblicke in mehrere Sicherheitsprodukte (Investigate, Enforcement, and CloudLock) und integriert diese in QRadar. Darüber hinaus kann der Benutzer die Sicherheit automatisieren und Bedrohungen schneller und direkt von QRadar aus eindämmen.

Wenn Sie die Cisco Cloud Security-App für QRadar einrichten, werden alle Daten der Cisco Cloud Security-Plattform integriert, und Sie können die Daten in grafischer Form in der QRadar-Konsole anzeigen. Mithilfe der Anwendung können Analysten:

- Untersuchen von Domänen, IP-Adressen, E-Mail-Adressen
- Sperren und Aufheben der Blockierung von Domänen (Durchsetzung)
- Informationen zu allen Vorfällen im Netzwerk anzeigen.

In diesem Artikel wird erläutert, wie Sie QRadar einrichten und ausführen, damit Sie die Protokolle aus Ihrem S3-Eimer abrufen und verbrauchen können.

Anforderungen



Anmerkung: QRadar wird von IBM unterstützt, da Cisco keinen direkten Support für Hardware oder Software von Drittanbietern leistet. Bei Problemen, die Ihr Umbrella Dashboard mit Ihrem S3-Bucket verbinden, können wir Sie unterstützen. Viele der hier aufgeführten Informationen sind auch auf der IBM-Website zu finden: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umb

Cisco Umbrella-Anforderungen

In diesem Dokument wird davon ausgegangen, dass Ihr Amazon AWS S3-Bucket in Umbrella (Einstellungen > Protokollverwaltung) konfiguriert wurde und grün angezeigt wird, nachdem die letzten Protokolle hochgeladen wurden.

Weitere Informationen zum Konfigurieren dieser Funktion finden Sie hier: Verwalten von Protokollen.

IBM Security QRadar SIEM-Anforderungen

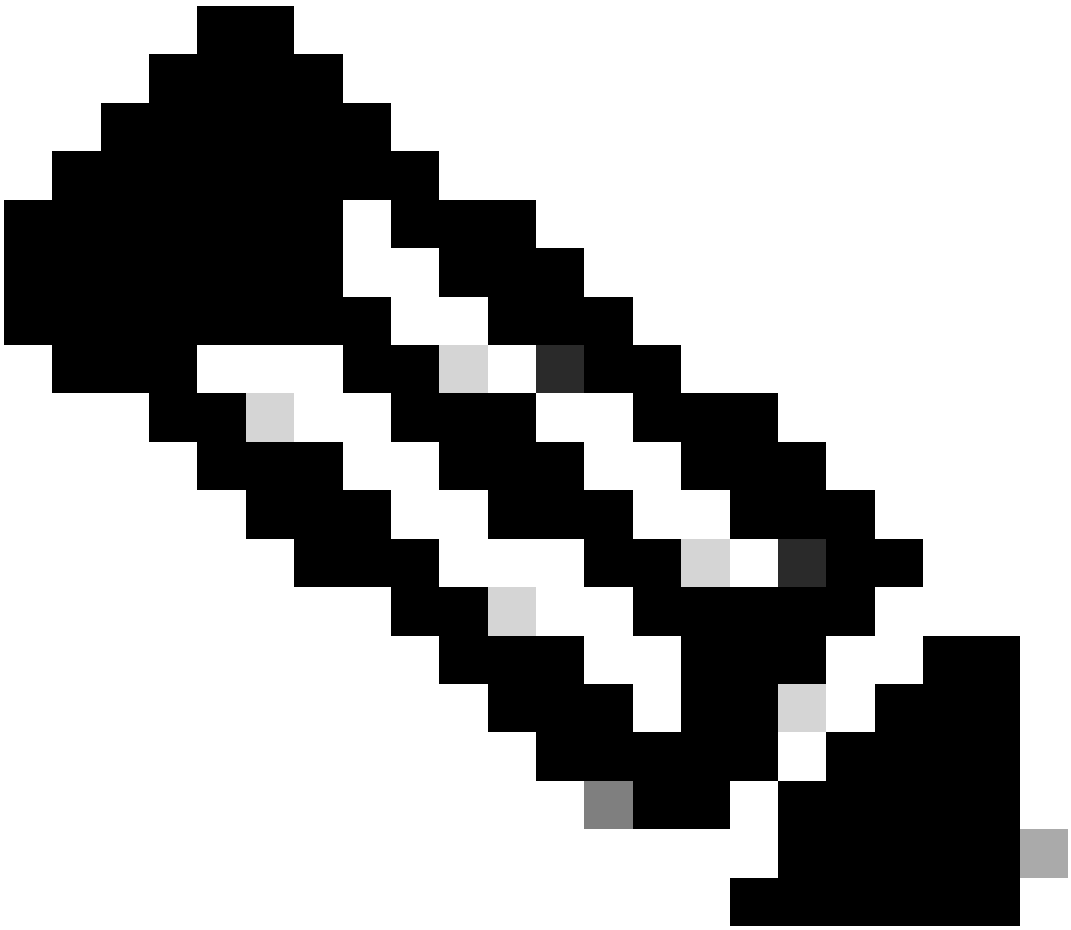
Der Administrator muss über Administratorrechte für die QRadar-Appliance(s), die Amazon S3-Konfiguration und das Umbrella Dashboard verfügen. Diese Anweisungen setzen voraus, dass der QRadar-Administrator mit der Erstellung von LSX-Dateien (Log Source Extension) vertraut ist.

Beachten Sie, dass die Cisco Cloud Security App v1.0.3 nur mit IBM QRadar 7.2.8 funktioniert. Die neue Version v1.0.6 arbeitet mit der aktuellen QRadar-Version ab 7.4.2.

Installation der Cisco Cloud Security App für IBM QRadar

1. Laden Sie die Cisco Cloud Security App für IBM QRadar herunter, und installieren Sie sie: Cisco Cloud Security App v1.0.3 (für IBM QRadar v7.2.8) oder Cisco Cloud Security App v1.0.6 (für IBM QRadar v7.4.8).
2. Nach der Installation können Sie Änderungen in QRadar bereitstellen.

Konfiguration der Cisco Cloud Security-App: Protokollquelle wird hinzugefügt

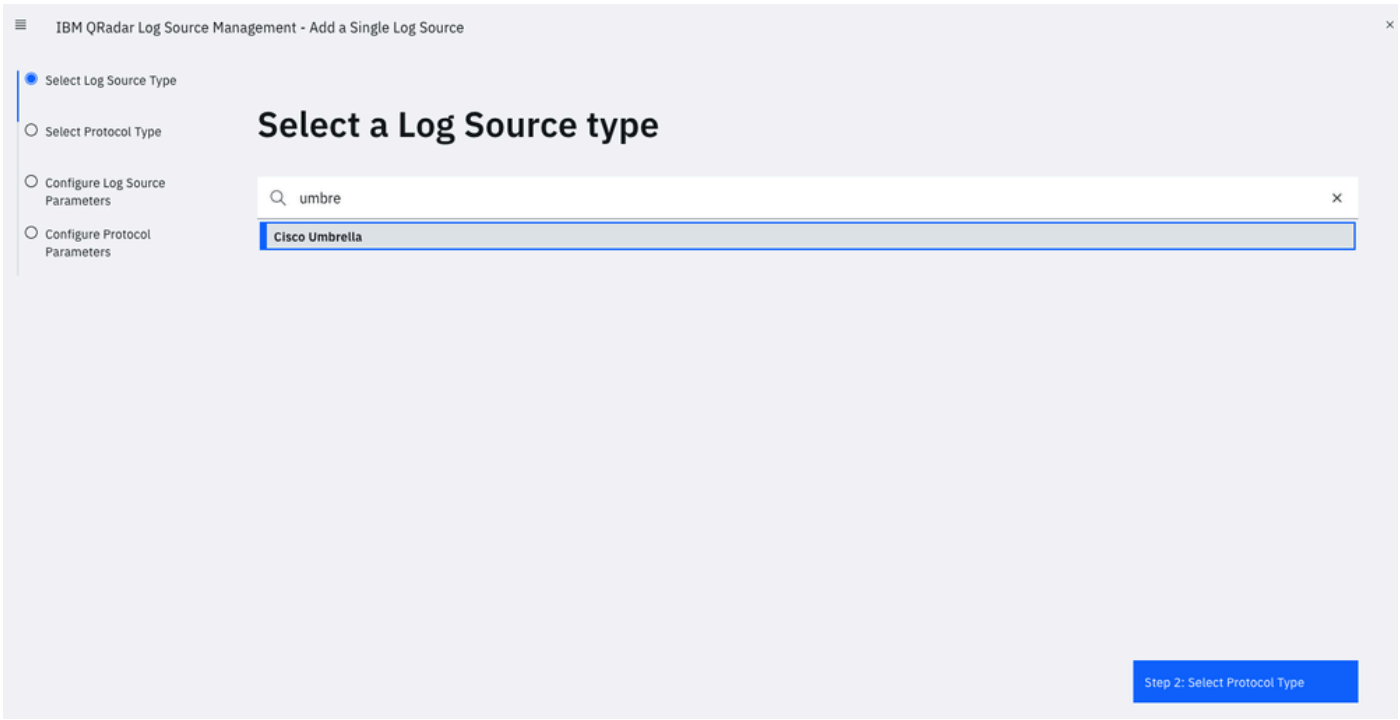


Anmerkung: Sie können andere Protokolle in S3 wie Audit und Firewall sehen, aber sie werden nicht unterstützt. Richten Sie nur die hier aufgeführten drei Geräte ein. Alle Versuche, diese anderen Protokolle zu konfigurieren, führen zu Fehlern.

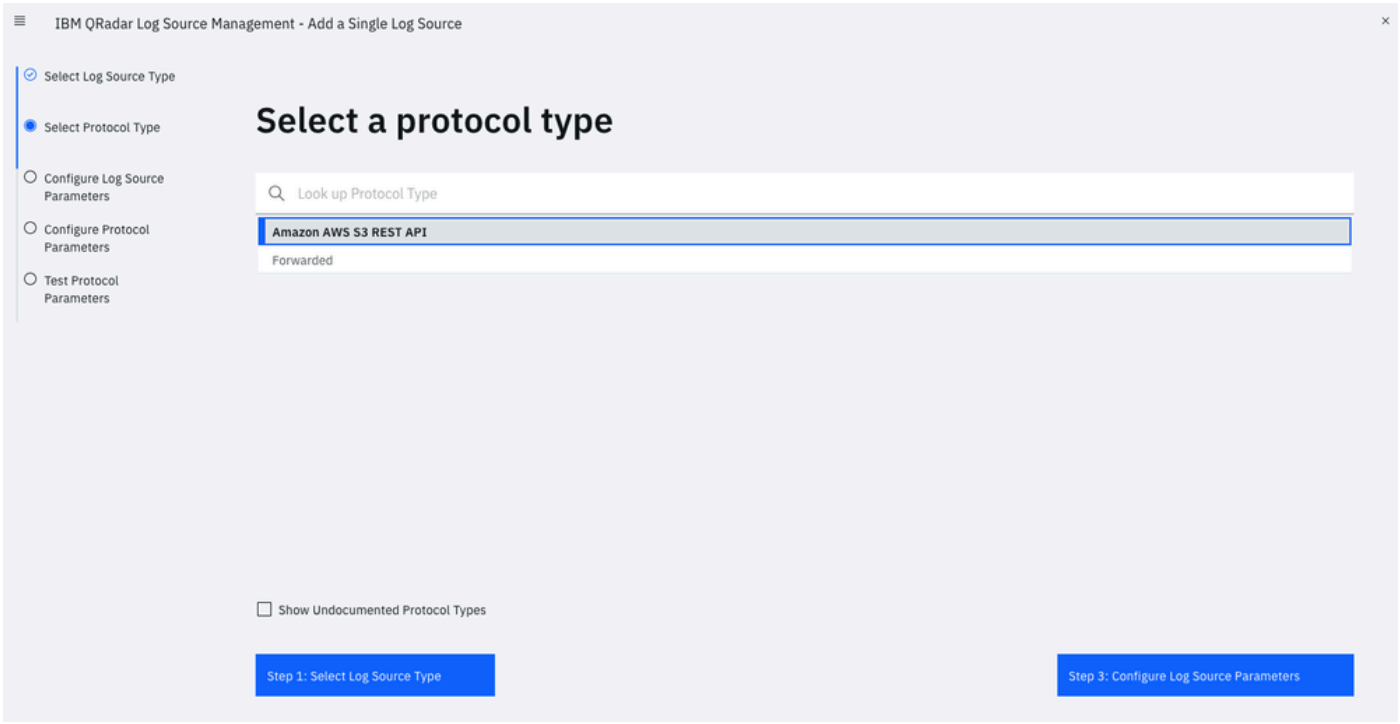
Um eine Protokollquelle hinzuzufügen, klicken Sie auf die Registerkarte Admin in der QRadar-Navigationsleiste, scrollen Sie nach unten und klicken Sie auf QRadar Log Source Management, dann klicken Sie auf die Schaltfläche +Neue Protokollquelle:

- Name der Protokollquelle (die Eintragsnamen müssen genau den aufgeführten übereinstimmen):
  - Cisco DNS-Protokolle: cisco_umbrella_dns_logs
  - Cisco Umbrella IP-Protokolle: cisco_umbrella_ip_logs
  - Cisco Umbrella Proxy-Protokolle: Cisco Umbrella Proxy-Protokolle
- Veranstaltungsformat: Cisco Umbrella CSV
- Protokollquellentyp: Cisco Umbrella
- Protokollkonfiguration: Amazon AWS S3 REST-API
- Dateimuster: .*?\.csv\.gz
- Protokollquellenerweiterung: CiscoUmbrella_ext **
- Wählen Sie alle Gruppen aus, denen diese Protokollquelle angehören soll: cisco_umbrella_logsource_group

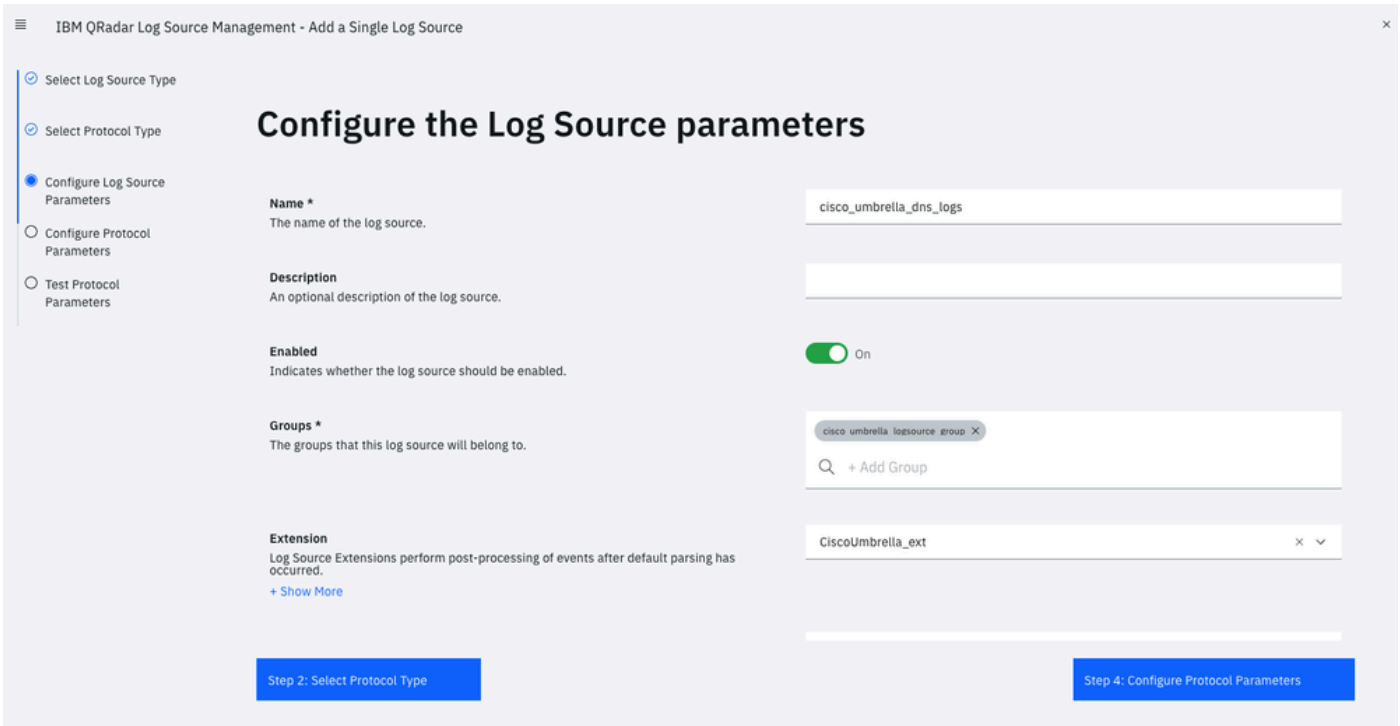
Gehen Sie durch den Assistenten zum Hinzufügen einer einzelnen Protokollquelle:



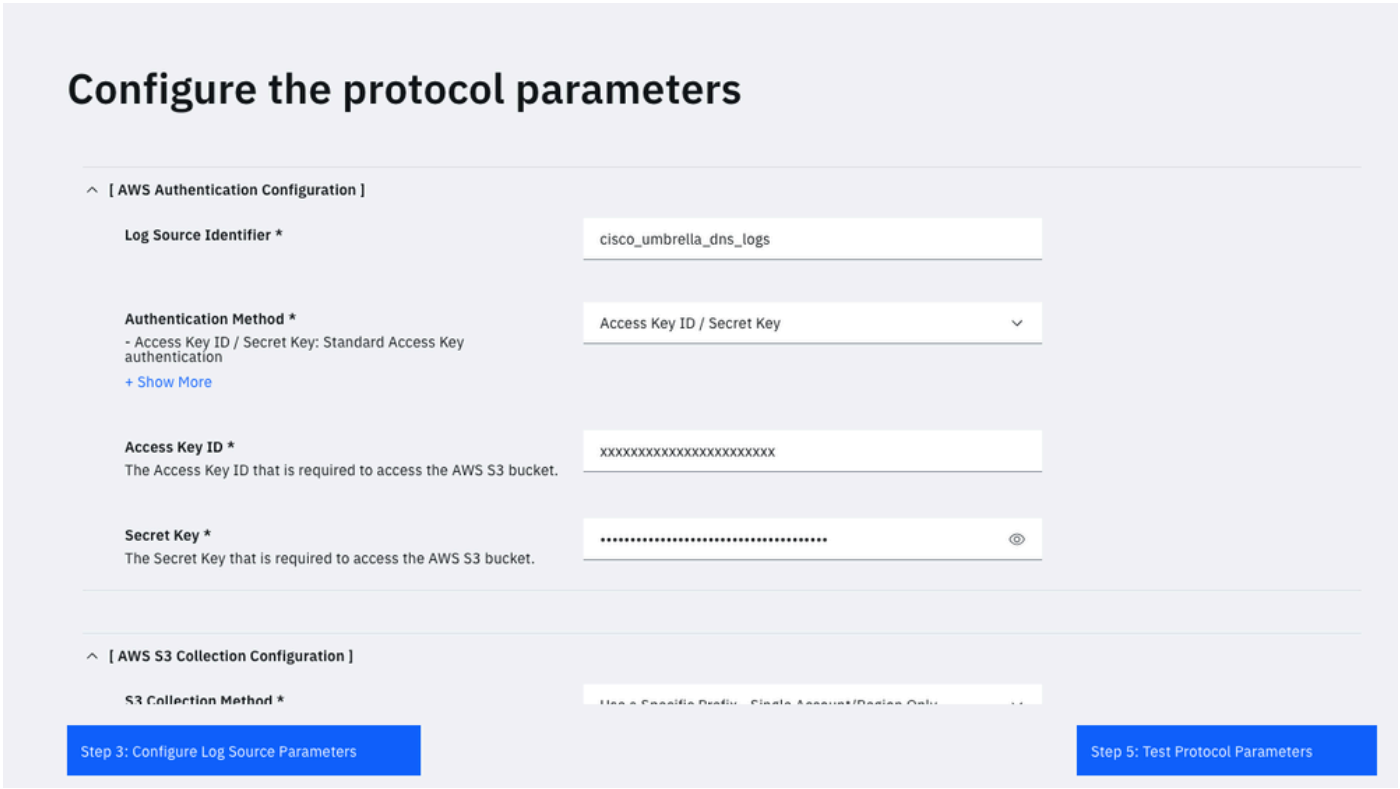
4404306773524



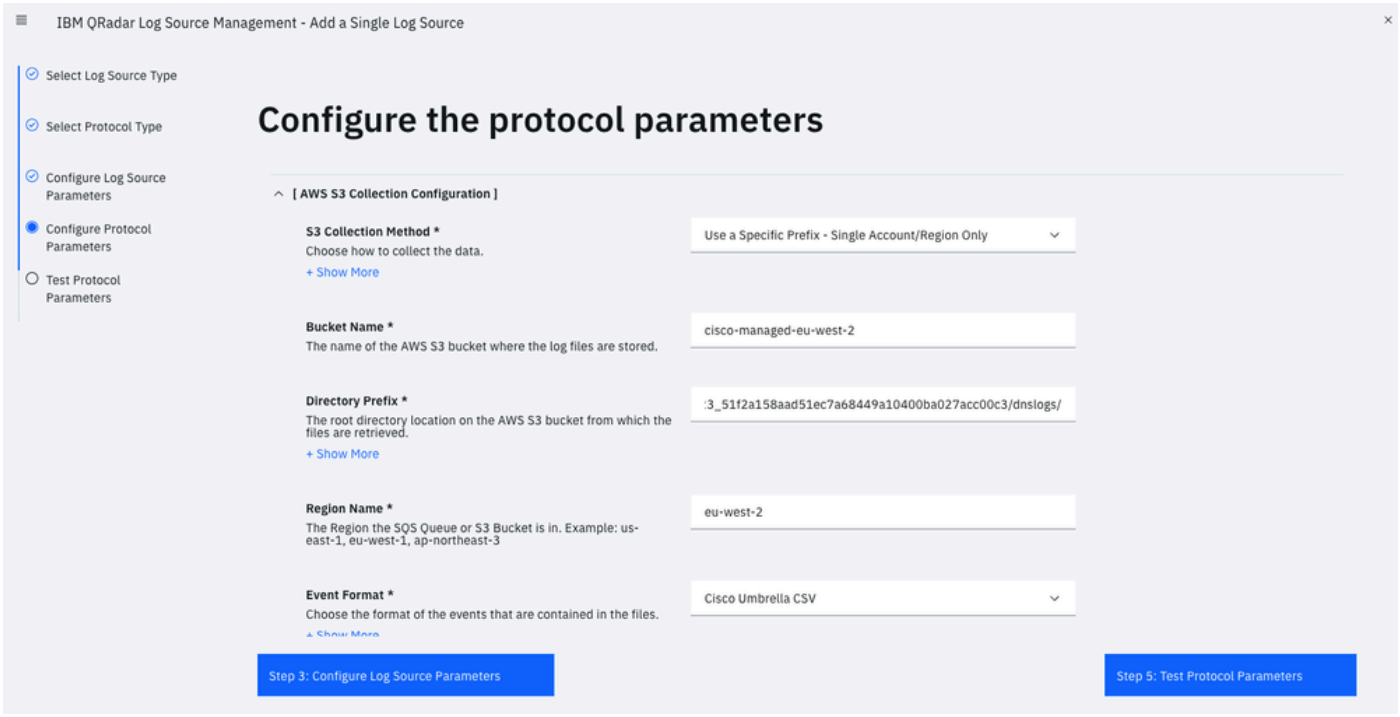
4404306773268



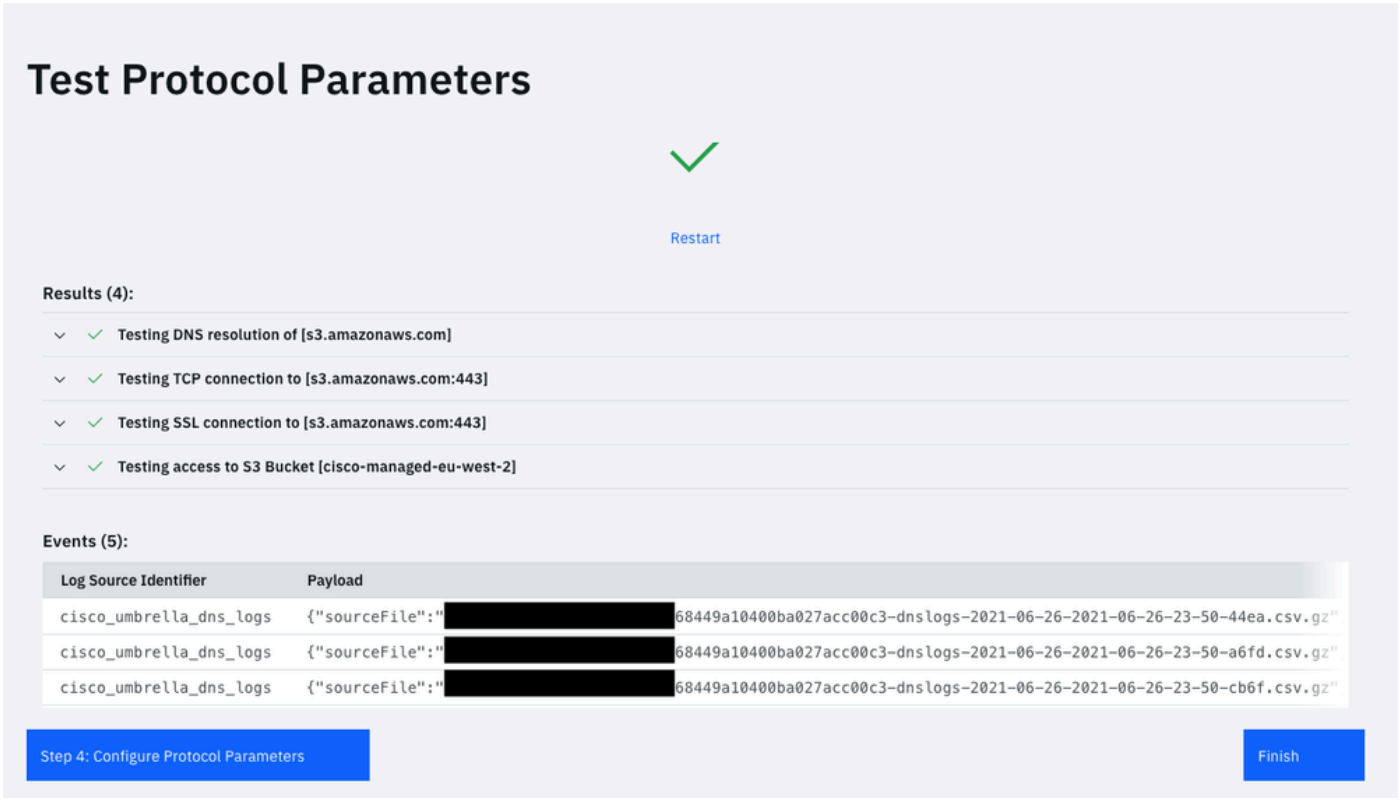
4404313505300



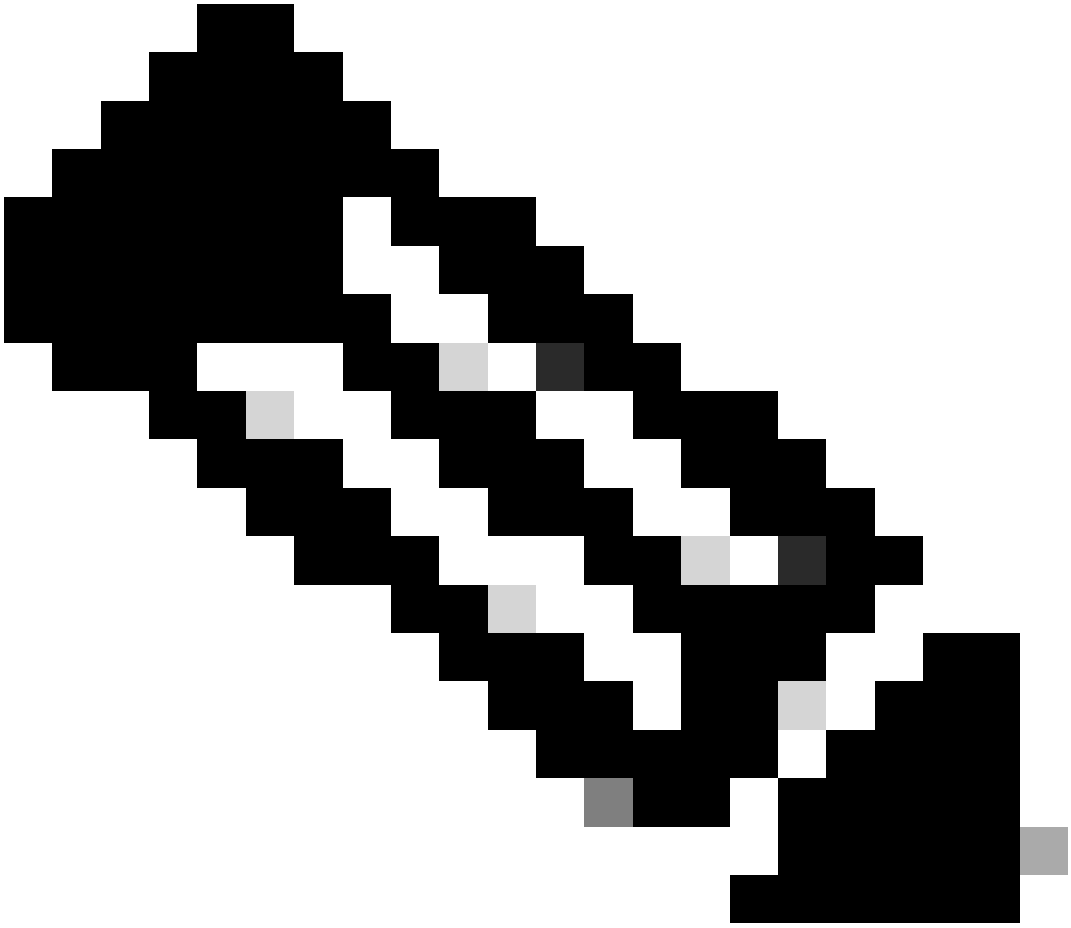
4404306774164



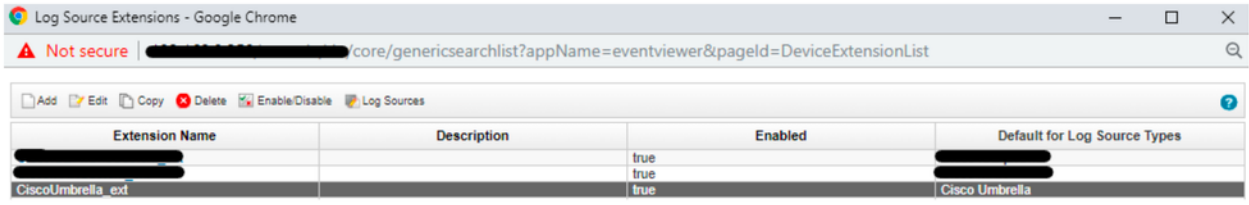
4404306897556



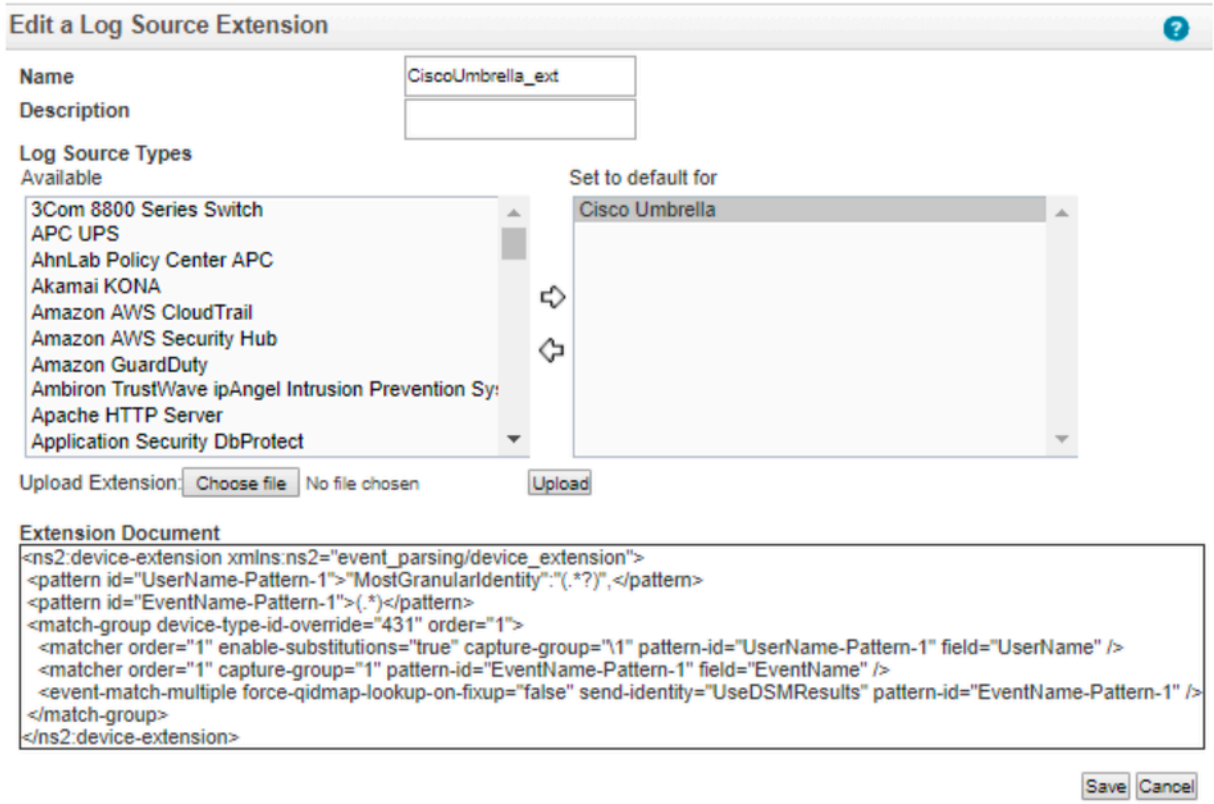
4404306881812



Anmerkung: Wenn die Protokollquellenerweiterung nicht "CiscoUmbrella_ext" zugeordnet ist, wählen Sie den Protokollquellennamen aus der Liste aus:



360071157752



360071326791

Das nachfolgende Beispiel zeigt das Aussehen eines Cisco Managed Buckets:

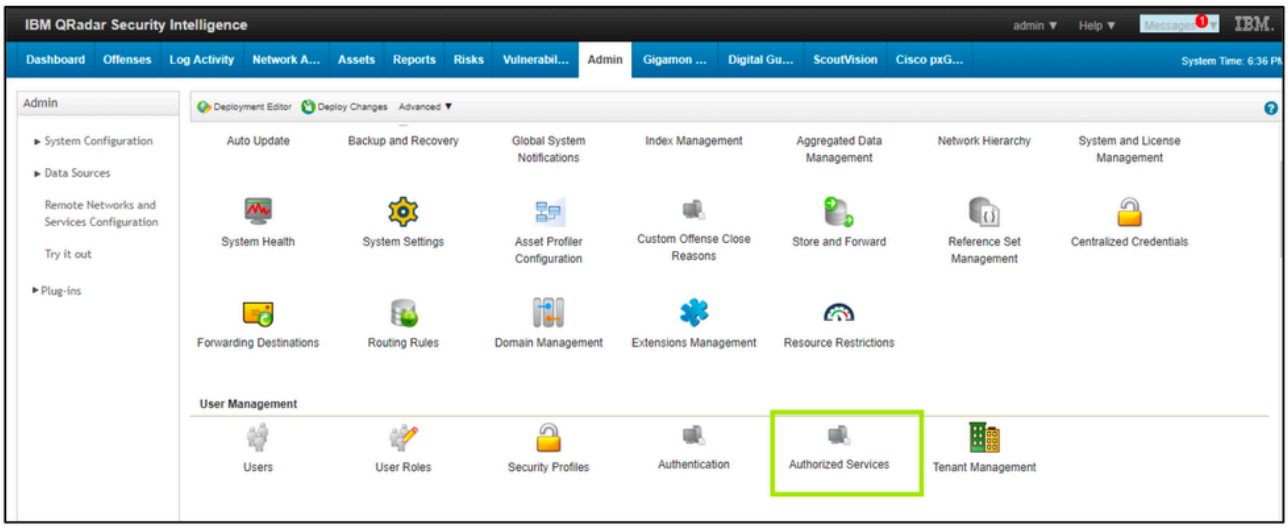
```
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxxx/dnslogs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

Navigieren Sie zurück zu den Cisco Cloud Security-App-Einstellungen, und stellen Sie die Aktualisierungsrate des Bereichs in Stunden auf den Mindestwert "1" ein, damit die Diagramme Daten anzeigen.

Authentifizierungstoken wird generiert

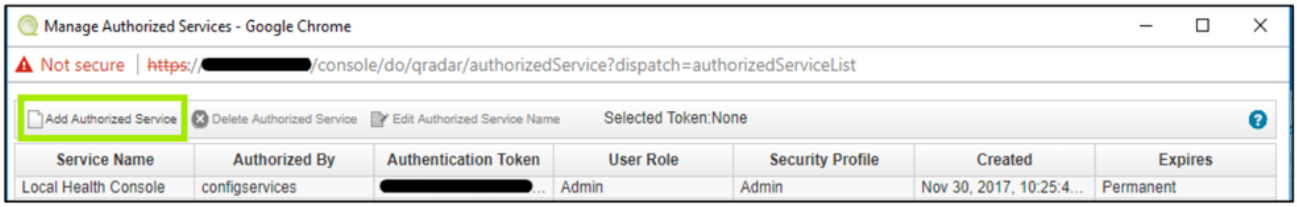
Der Administrator muss ein Service-Token generieren, um es Ihrer Cisco Security-App hinzuzufügen. Als Best Practice wurde das Authorized Service Token alle 90 Tage neu erstellt:

1. Melden Sie sich bei QRadar > Registerkarte Admin > Authorized Services an.



360071965571

2. Autorisierte Services hinzufügen

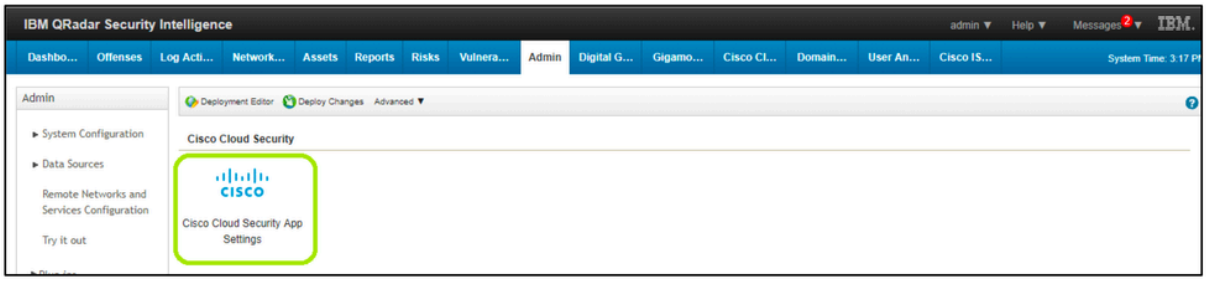


360071965551

3. Geben Sie die Details ein, und generieren Sie ein Authentifizierungstoken.
4. Nachdem Sie das Token generiert haben, klicken Sie auf "Deploy Changes".

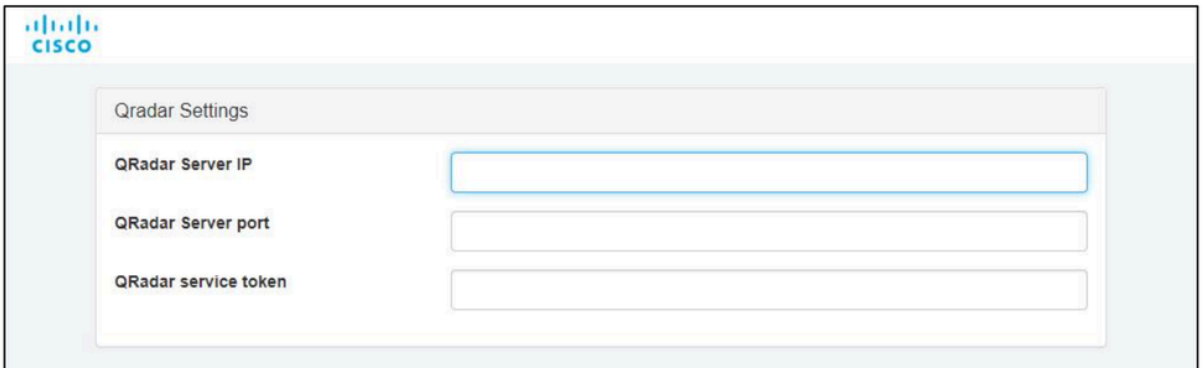
Konfigurieren der Cisco Cloud Security-App

1. Scrollen Sie von der Registerkarte Admin in der QRadar-Navigationsleiste nach unten, und öffnen Sie die Einstellungen der Cisco Cloud Security-App.



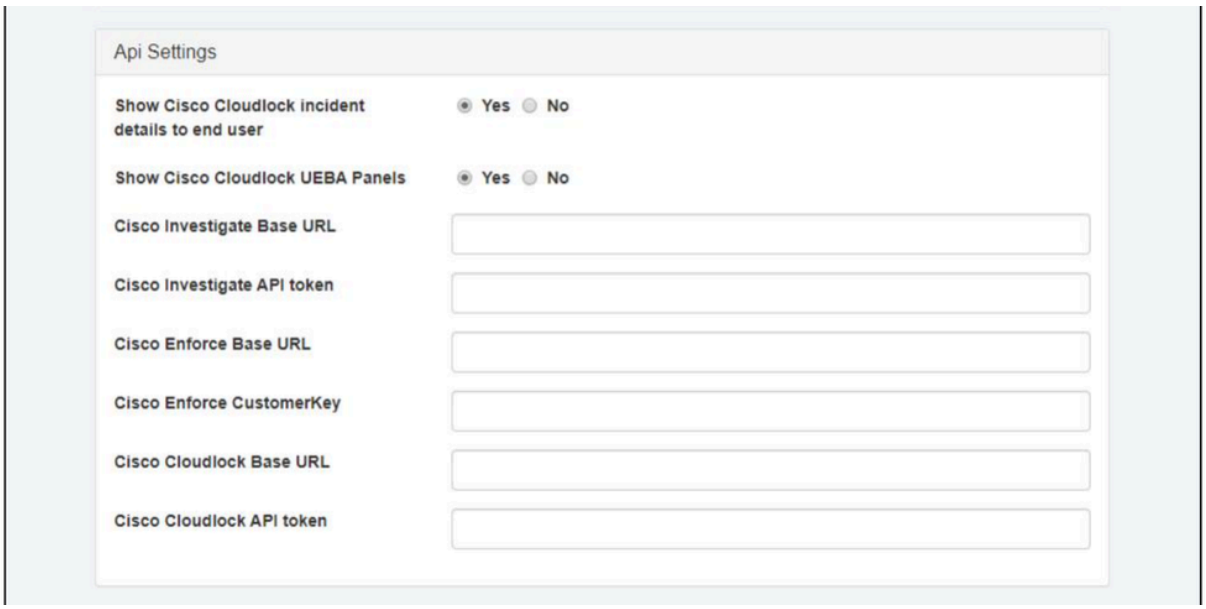
360071754732

2. Geben Sie das im vorherigen Schritt generierte Authentifizierungstoken ein.



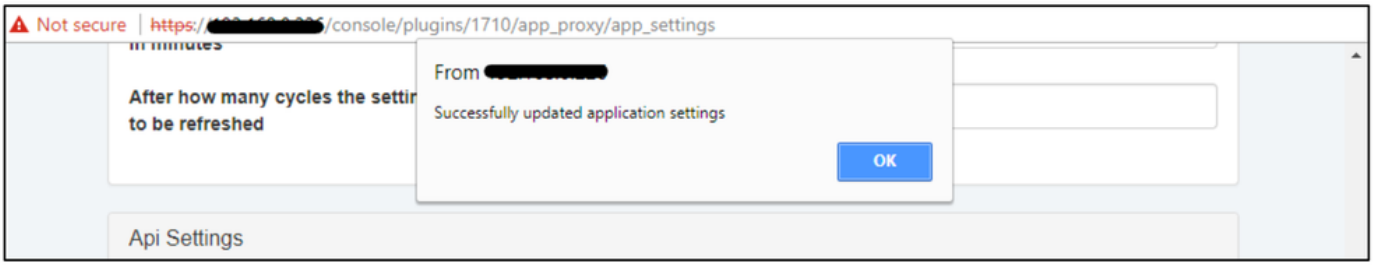
360072462992

3. Bearbeiten Sie die API-Einstellungen wie folgt:
    - URL der Cisco Investigate Base: https://investigate.api.umbrella.com/
    - Cisco Investigate API-Token: Generieren über das Umbrella Dashboard -> Investigate -> API Keys -> Create New Token; Weitere Informationen finden Sie unter https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key
    - Basis-URL für Cisco Enforce: https://s-platform.api.opendns.com/1.0/
    - Cisco Kundenschlüssel durchsetzen: Generierung über das Umbrella Dashboard -> Richtlinienkomponenten -> Integrationen -> Hinzufügen; Weitere Informationen finden Sie unter https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations
    - Cisco Cloudlock Base-URL: https://{YourCloudlockAPIServer}/api/v2 (z. B. https://api-demo.cloudlock.com/api/v2/. Bitte bestätigen Sie Ihre Cloudlock Base-URL, auch Cloudlock Enterprise API-URL genannt, per E-Mail an support@cloudlock.com.)
    - Cisco Cloudlock API-Token: via Cloudlock generieren -> Einstellungen -> Authentifizierung & API -> Generieren; Weitere Informationen finden Sie unter https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication



360072703611

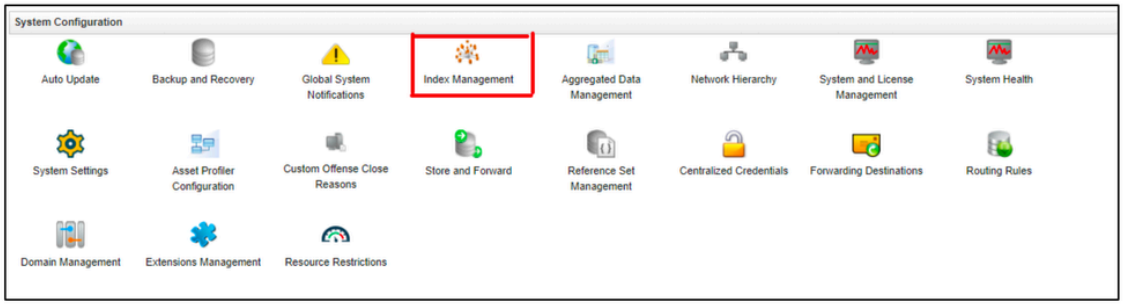
Ein Popup zeigt an, dass die Anwendungseinstellungen erfolgreich aktualisiert wurden.



360071986151

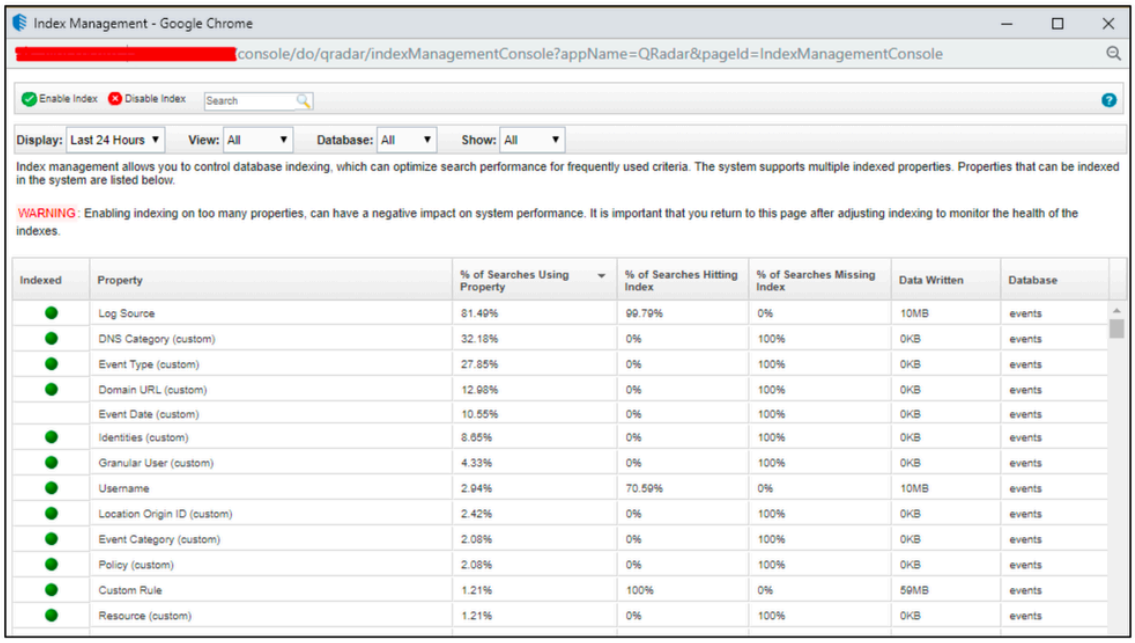
Indizierung in QRadar

1. Navigieren Sie zur Registerkarte Admin, und klicken Sie dann auf Indexverwaltung.



360071780112

2. Indizieren Sie die mit der App verpackten CEPs.



360071988811

Die folgenden CEPs werden für die Indizierung empfohlen:

1. Protokollquelle
2. DNS-Kategorie
3. Ereignistyp
4. Domänen-URL
5. Identitäten
6. Detaillierter Benutzer
7. Benutzername
8. Standort-Ursprungs-ID
9. Ereigniskategorie
10. Richtlinie
11. Ressource

Jetzt können Sie mit QRadar die Überwachung von Details zu Cisco Umbrella, Investigate und CloudLock starten. Weitere Anweisungen zur Navigation in QRadar finden Sie hier: Navigation in der Cisco Cloud Security App

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.