Configurazione dell'app Cloud Security per IBM QRadar

Sommario

Introduzione

In questo documento viene descritto come configurare l'app Cisco Cloud Security con IBM QRadar per l'analisi dei log.

Panoramica

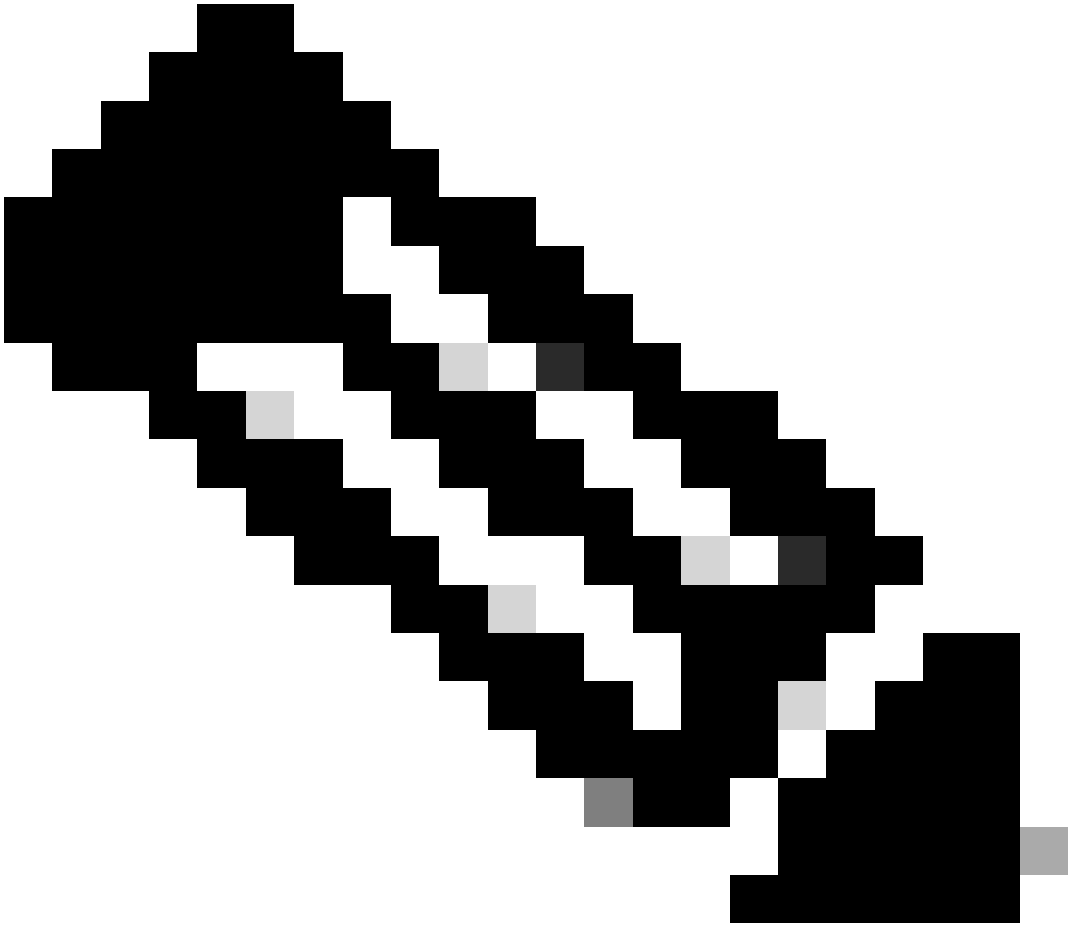
QRadar di IBM è un popolare SIEM per l'analisi dei log. Fornisce una potente interfaccia per l'analisi di grandi blocchi di dati, ad esempio i registri forniti da Cisco Umbrella per il traffico DNS della tua organizzazione. Cisco Cloud Security App per IBM QRadar offre informazioni dettagliate su più prodotti di sicurezza (Investigate, Enforcement e CloudLock) e li integra con QRadar. Consente inoltre all'utente di automatizzare la sicurezza e contenere le minacce in modo più rapido e diretto da QRadar.

Quando si configura l'app Cisco Cloud Security per QRadar, integra tutti i dati della piattaforma Cisco Cloud Security e consente di visualizzare i dati in formato grafico nella console QRadar. Dall'applicazione, gli analisti possono:

- Analizza domini, indirizzi IP, indirizzi e-mail
- Bloccare e sbloccare i domini (imposizione)
- Visualizzare le informazioni di tutti gli incidenti della rete.

Questo articolo descrive le procedure di base per la configurazione e l'esecuzione di QRadar in modo che possa estrarre i registri dal secchio S3 e utilizzarli.

Requisiti



Nota: Il supporto per QRadar deve provenire da IBM, in quanto Cisco non è in grado di supportare direttamente hardware o software di terze parti. Per qualsiasi problema di collegamento del dashboard Umbrella al secchio S3, Dell può fornire assistenza. Molte delle informazioni reperibili qui sono reperibili anche sul sito web di IBM: https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umb

Requisiti di Cisco Umbrella

In questo documento si presume che il bucket S3 di Amazon AWS sia stato configurato in Umbrella (Impostazioni > Gestione log) e sia visualizzato in verde con i log recenti caricati.

Per ulteriori informazioni su come configurare questa funzione, vedere: Gestione dei log.

Requisiti SIEM per IBM Security QRadar

L'amministratore deve disporre di diritti amministrativi per gli accessori QRadar, la configurazione Amazon S3 e il dashboard Umbrella. In base a queste istruzioni, l'amministratore QRadar ha

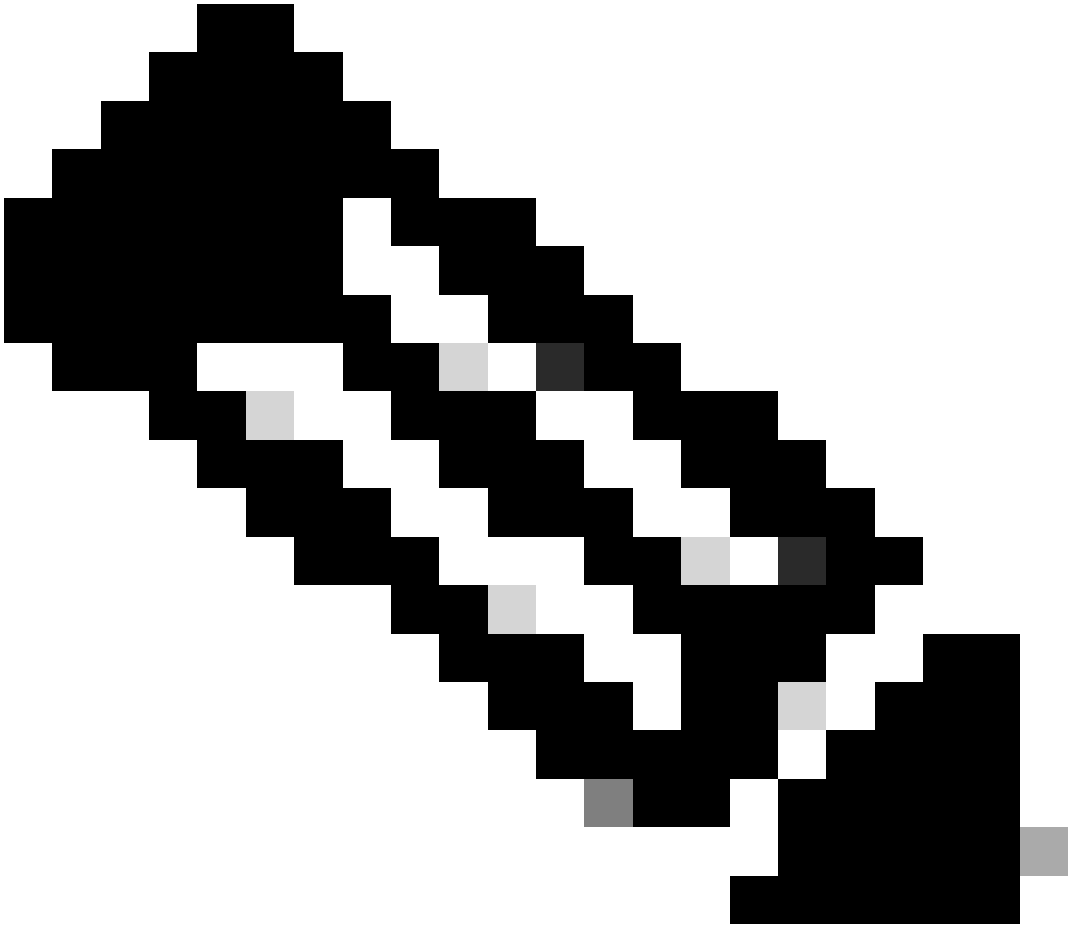
familiarità con la creazione di file LSX (Log source Extension).

Tenere presente che Cisco Cloud Security App v1.0.3 funziona solo con IBM QRadar 7.2.8. La nuova versione, v1.0.6, funziona con l'attuale versione QRadar dalla 7.4.2 e successive.

Installazione di Cisco Cloud Security App per IBM QRadar

1. Scaricare e installare Cisco Cloud Security App per IBM QRadar, disponibile qui: Cisco Cloud Security App v1.0.3 (per IBM QRadar v7.2.8) o Cisco Cloud Security App v1.0.6 (per IBM QRadar v7.4.8).
2. Dopo l'installazione, distribuire le modifiche in QRadar.

Configurazione app Cisco Cloud Security: Aggiunta dell'origine del log



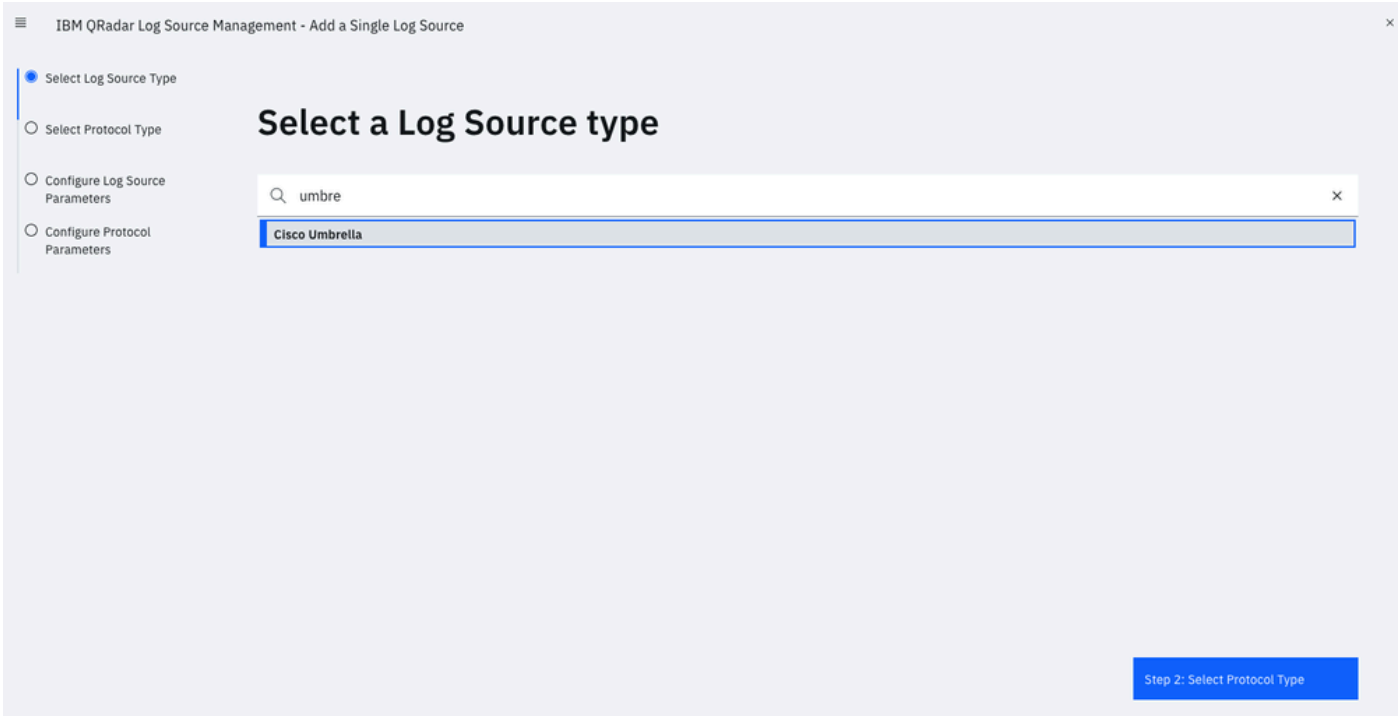
Nota: In S3 è possibile visualizzare altri log, ad esempio Audit e Firewall, ma questi non

sono supportati. Impostare solo i tre elencati qui. Qualsiasi tentativo di configurare gli altri registri genera un errore.

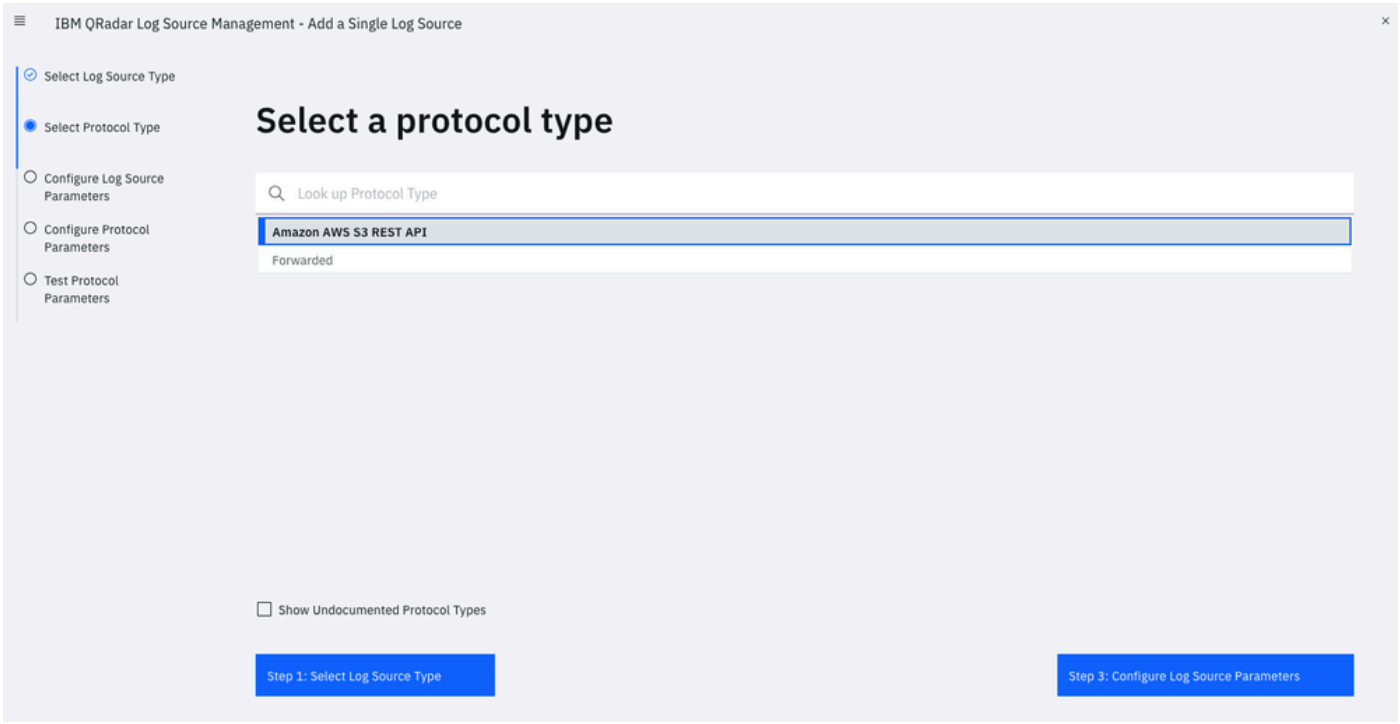
Per aggiungere un'origine registro, fare clic sulla scheda Admin sulla barra di navigazione QRadar, scorrere verso il basso e fare clic su QRadar Log Source Management, quindi fare clic sul pulsante +New Log Source:

- Nome origine log (i nomi delle voci devono corrispondere esattamente a quelli elencati):
  - Registri DNS Cisco: log_ombrello_dns_cisco
  - Log IP di Cisco Umbrella: cisco_umbrella_ip_logs
  - Registri proxy Cisco Umbrella: log_ombrello_proxy_cisco
- Formato evento: Cisco Umbrella CSV
- Tipo origine registro: Cisco Umbrella
- Configurazione protocollo: API REST Amazon AWS S3
- Modello file: .*?\.csv\.gz
- Estensione origine registro: Cisco Umbrella_ext **
- Selezionare i gruppi di cui si desidera che l'origine registro sia membro: gruppo_origine_log_ombrello_cisco

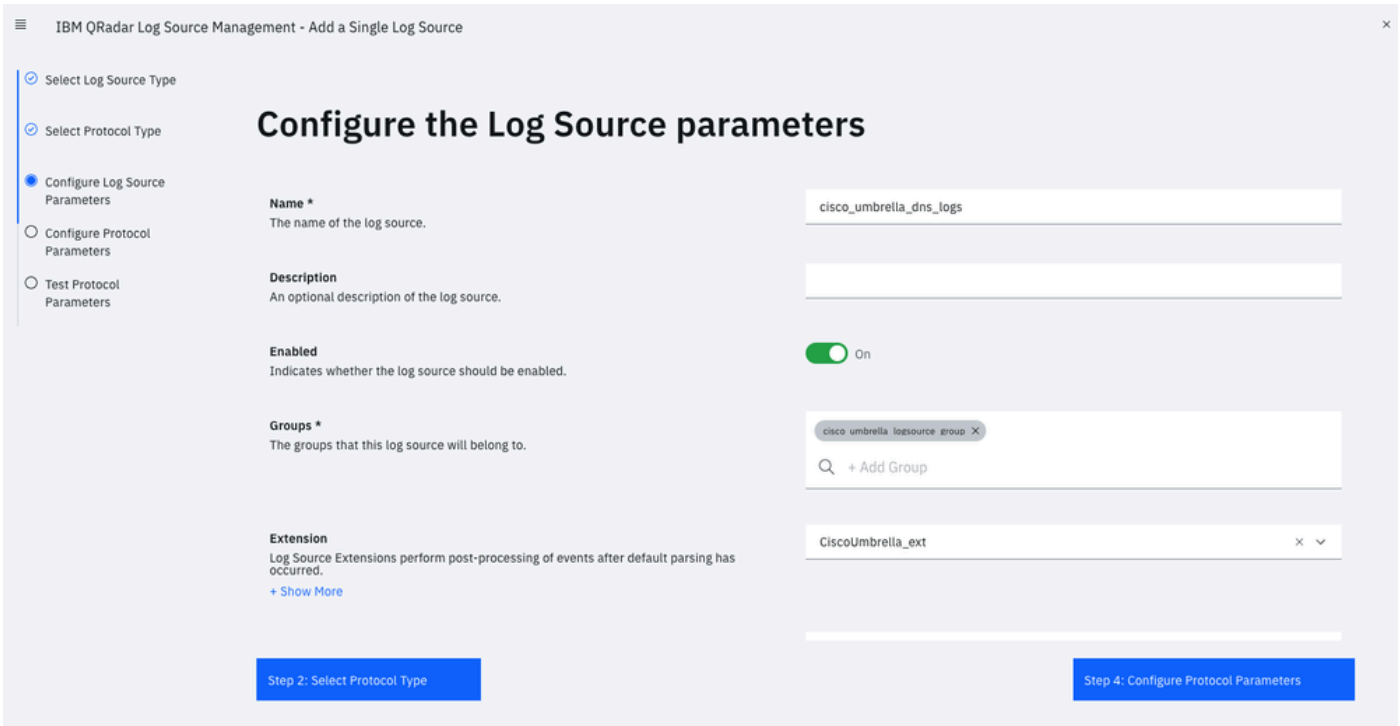
Per ulteriori informazioni, vedere Aggiunta guidata singola origine log:



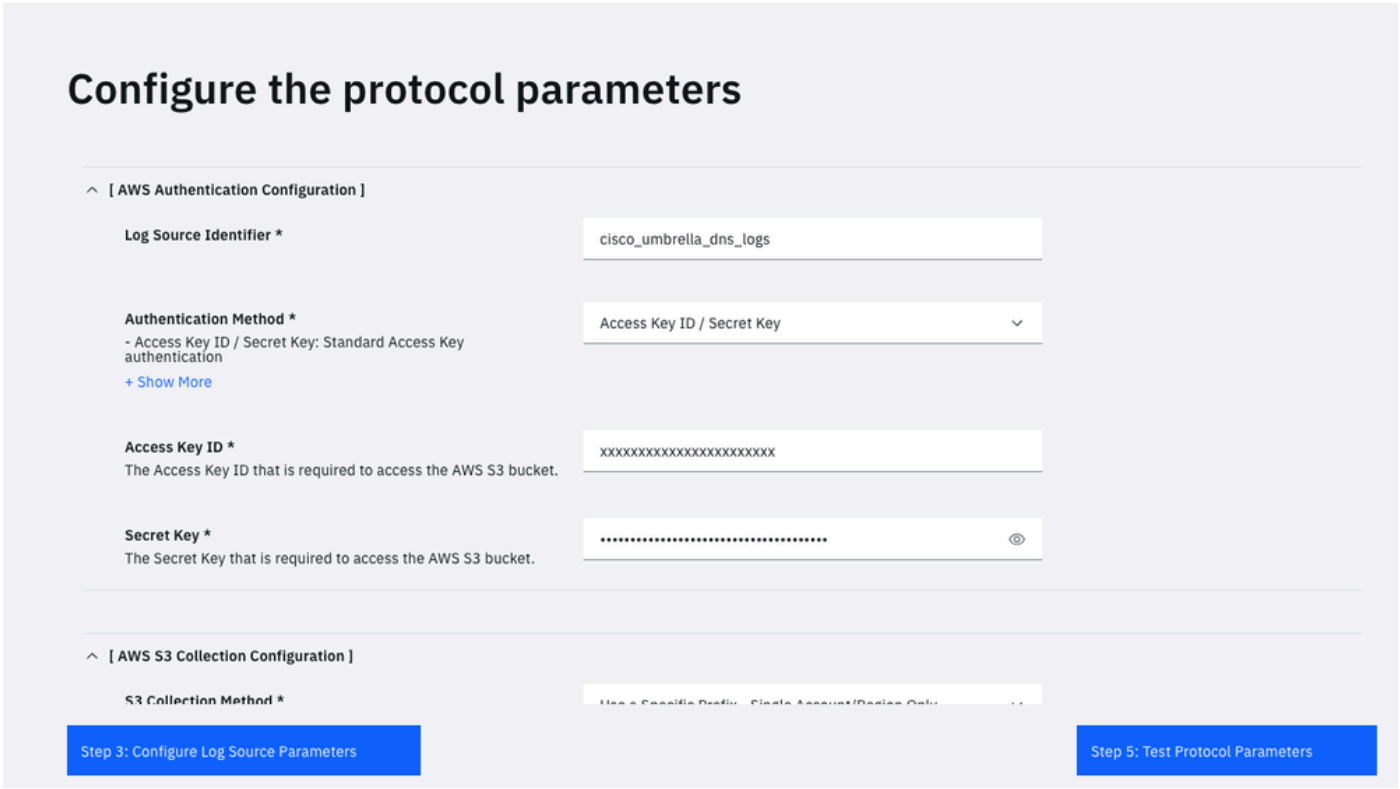
4404306773524



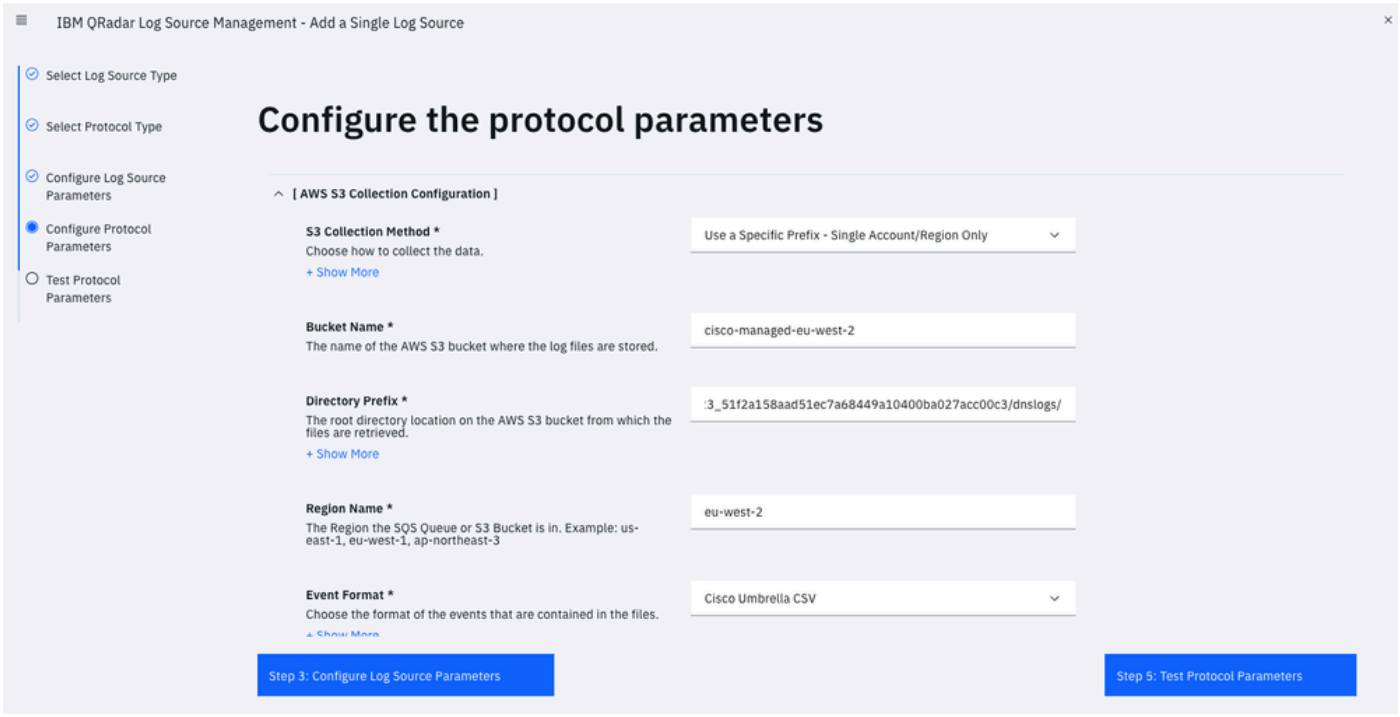
4404306773268



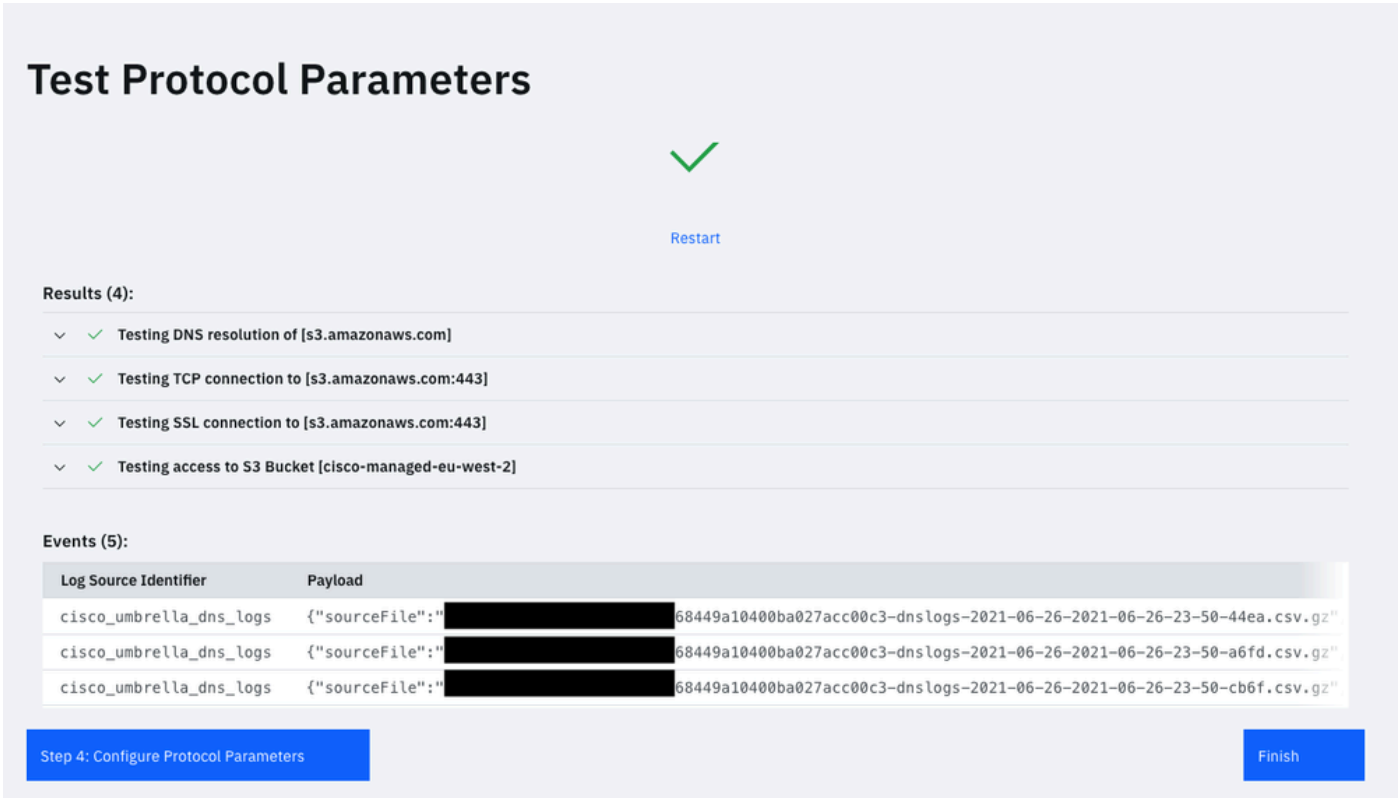
4404313505300



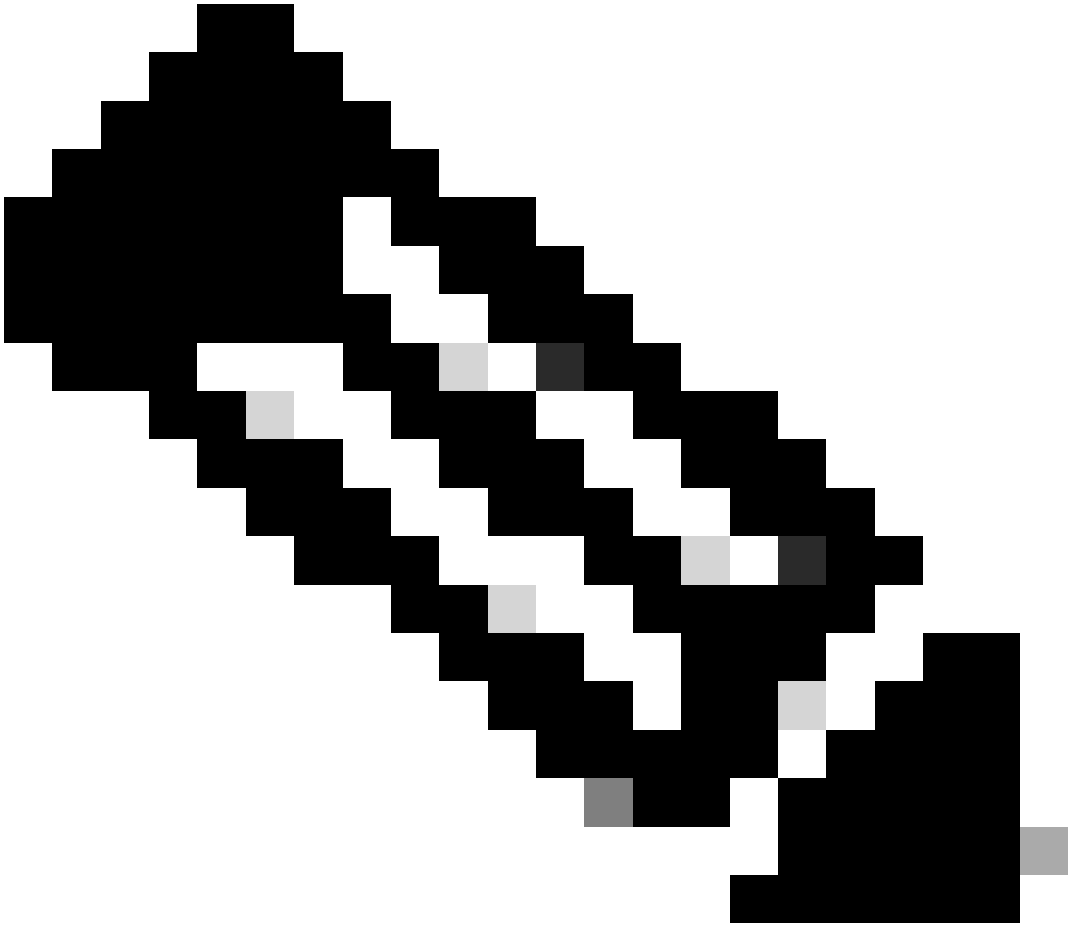
4404306774164



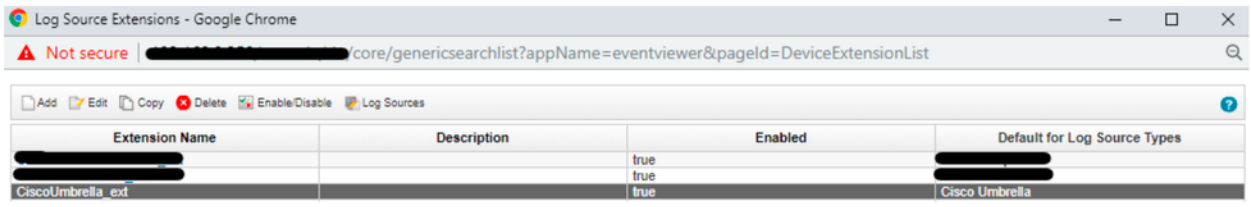
4404306897556



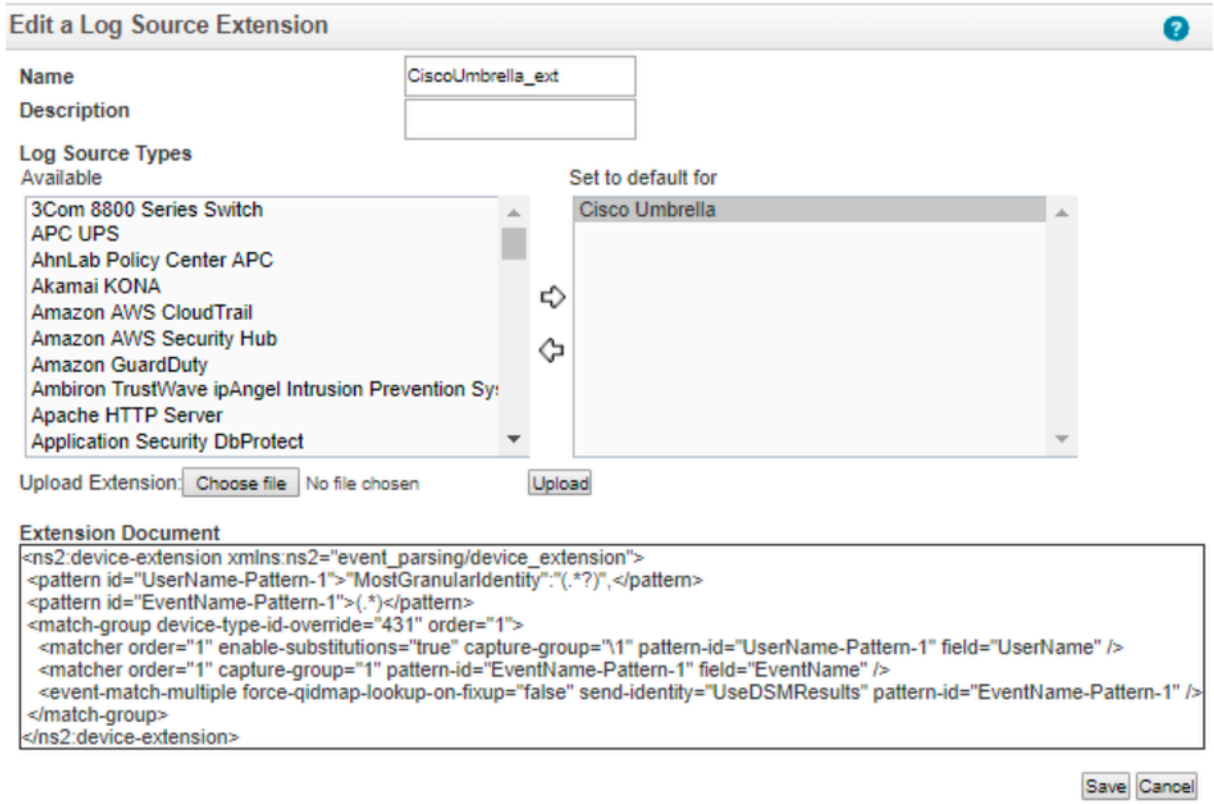
4404306881812



Nota: Se l'estensione dell'origine del log non è mappata a "CiscoUmbrella_ext", scegliere il nome dell'origine del log dall'elenco:



360071157752



360071326791

Di seguito è riportato un esempio di un bucket gestito da Cisco:

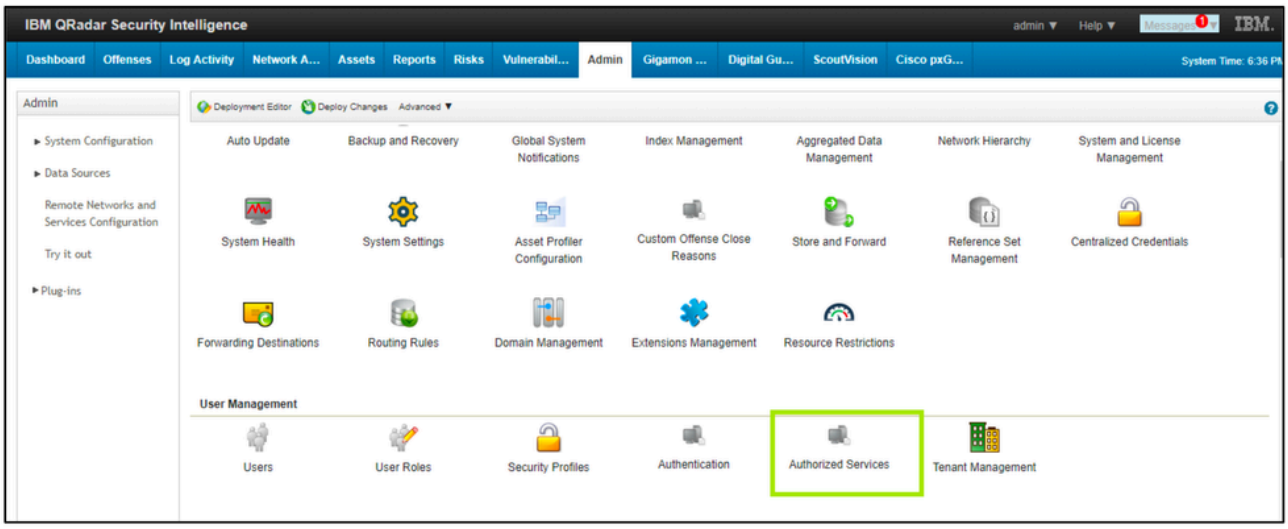
```
Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxxx/dnslogs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

Tornare a Cisco Cloud Security App Settings e impostare la frequenza di aggiornamento del pannello in ore su un valore minimo di "1" per consentire ai grafici di visualizzare i dati.

Generazione del token di autenticazione

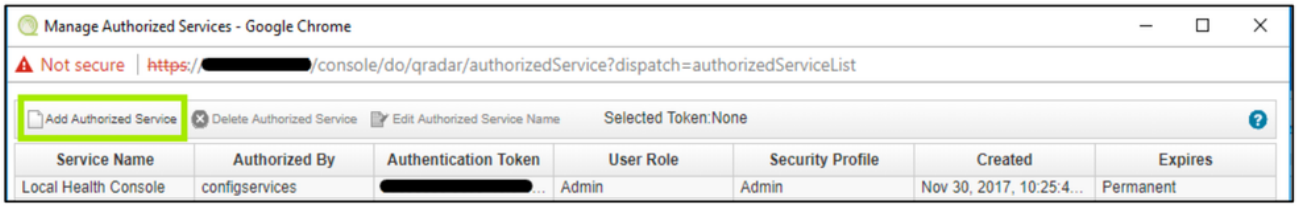
L'amministratore deve generare un token del servizio da aggiungere all'app Cisco Security. È buona norma ricreare il token del servizio autorizzato ogni 90 giorni:

1. Accedere a QRadar > Scheda Amministrazione > Servizi autorizzati.



360071965571

2. Aggiungere servizi autorizzati.

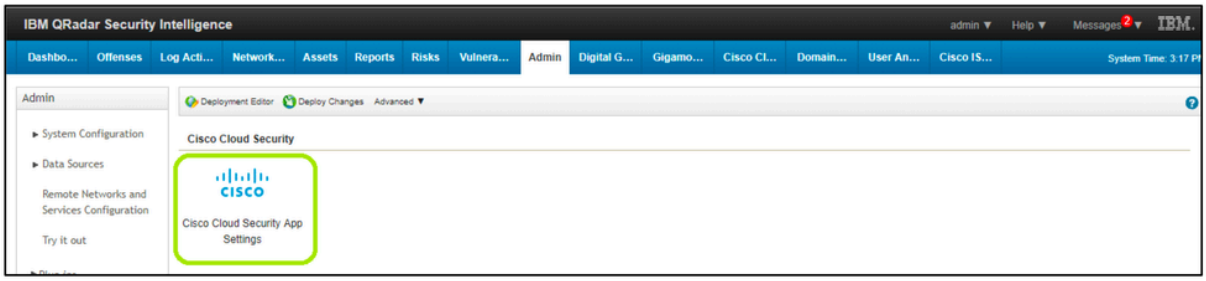


360071965551

3. Immettere i dettagli e generare il token di autenticazione.
4. Dopo aver generato il token, fare clic su "Deploy Changes" (Distribuisci modifiche).

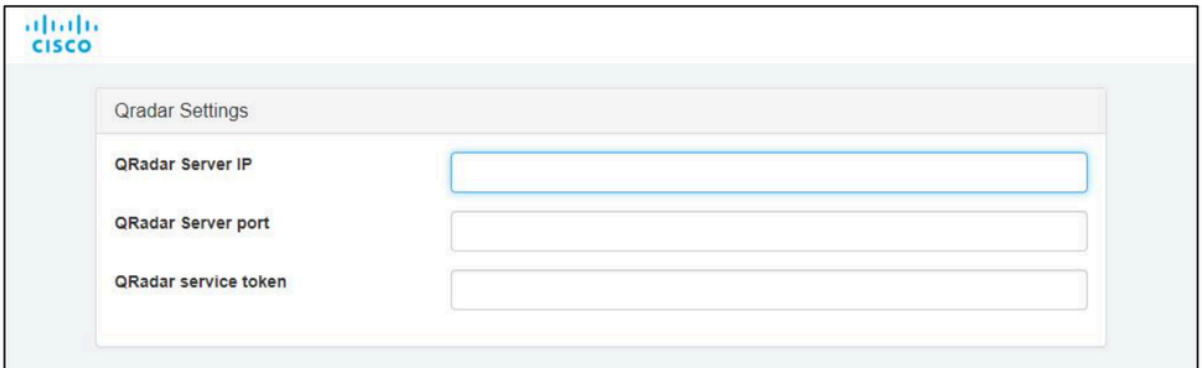
Configurazione dell'app Cisco Cloud Security

1. Dalla scheda Admin sulla barra di navigazione di QRadar, scorrere verso il basso e aprire Cisco Cloud Security App Settings.



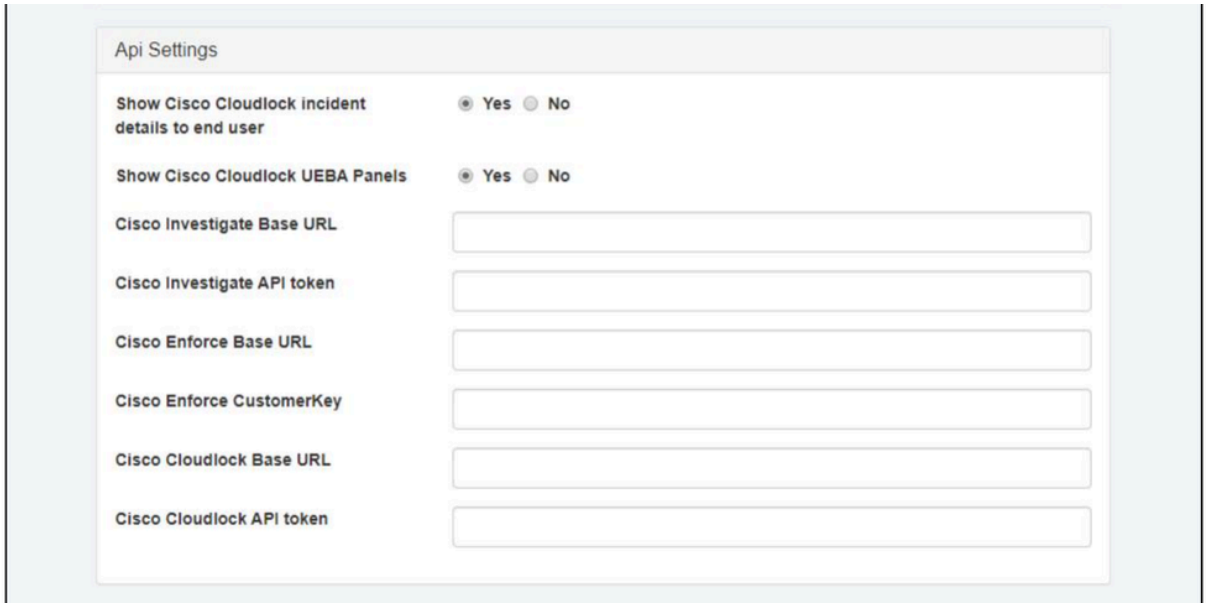
360071754732

2. Immettere il token di autenticazione generato nel passaggio precedente.



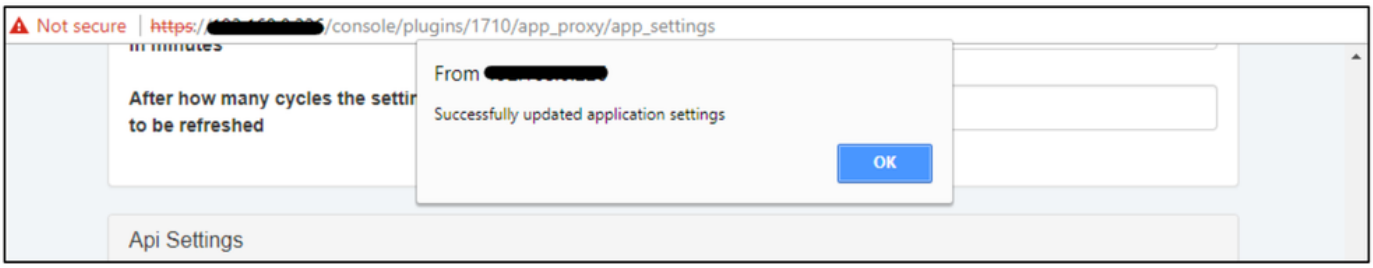
360072462992

3. Modificare le impostazioni dell'Api come segue:
    - URL di base investigazione Cisco: https://investigate.api.umbrella.com/
    - Token API Cisco Investigate: genera mediante il dashboard Umbrella -> Indaga -> Chiavi API -> Crea nuovo token; per ulteriori informazioni, visitare il sito https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key
    - URL di base Cisco Enforce: https://s-platform.api.opendns.com/1.0/
    - Cisco Enforce CustomerKey: genera mediante il dashboard Umbrella -> Componenti delle policy -> Integrazioni -> Aggiungi; per ulteriori informazioni, visitare il sito https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations
    - URL di base Cisco Cloudlock: https://{YourCloudlockAPIServer}/api/v2 (ad esempio, https://api-demo.cloudlock.com/api/v2/. Confermare l'URL di base Cloudlock o l'URL dell'API Cloudlock Enterprise inviando un'e-mail a support@cloudlock.com.)
    - Token API Cisco Cloudlock: generate via Cloudlock -> Settings -> Authentication & API -> Generate; per ulteriori informazioni, visitare il sito https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication



360072703611

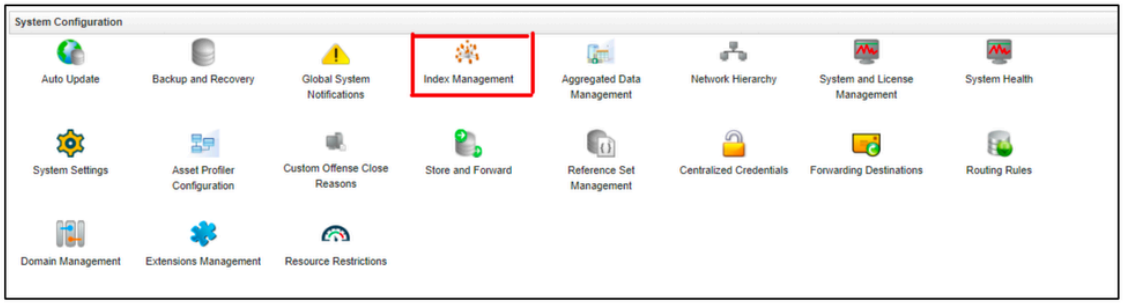
Un popup indica che le impostazioni dell'applicazione sono state aggiornate correttamente.



360071986151

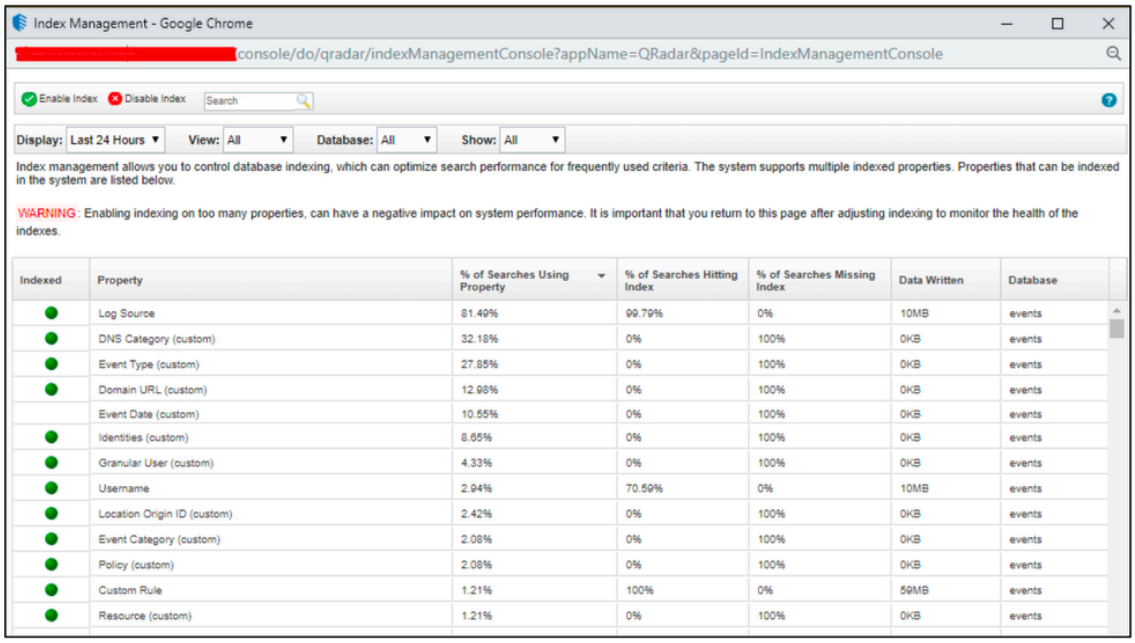
Indicizzazione in QRadar

1. Passare alla scheda Admin, quindi fare clic su Index Management (Gestione indici).



360071780112

2. Indicizza i CEP inseriti nel pacchetto con l'app.



360071988811

Di seguito sono riportati i CEP consigliati da indicizzare:

1. Origine registro
2. Categoria DNS
3. Tipo di evento
4. URL dominio
5. Identità
6. Utente granulare
7. Username
8. ID origine ubicazione
9. Categoria evento
10. Policy
11. Risorsa

A questo punto è possibile utilizzare QRadar per iniziare le attività di monitoraggio per i dettagli Cisco Umbrella, Investigate e CloudLock. Ulteriori istruzioni su come navigare in QRadar sono disponibili qui: Navigazione in Cisco Cloud Security App.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).