Usa l'API Umbrella Reporting tramite Postman

Sommario

Introduzione

Questo documento descrive come utilizzare l'API Cisco Umbrella Reporting in Postman.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

L'API Umbrella è stata rilasciata nel settembre 2022, fornendo una piattaforma sicura e facile da usare che consente agli utenti di costruire, estendere e integrare con Umbrella.

Gli endpoint dell'API Umbrella sono ospitati in api.umbrella.com, con percorsi raggruppati per caso di utilizzo. Le chiavi API possono essere gestite sia nel dashboard Umbrella, in Amministrazione > chiavi API, sia a livello di programmazione con l'API KeyAdmin. Ogni chiave può essere configurata in modo granulare con più ambiti raggruppati in cinque casi di utilizzo principali:

- Gli endpoint API di amministrazione consentono di eseguire il provisioning e gestire gli utenti

e le chiavi API Umbrella, visualizzare i ruoli e gestire i clienti per provider e provider gestiti.
- Gli endpoint API Auth consentono di autorizzare l'integrazione di altri servizi con la piattaforma Umbrella.
- Gli endpoint API di distribuzione consentono di eseguire il provisioning, il monitoraggio e la gestione di reti e altre entità diverse e di proteggerle configurandole nei criteri Umbrella esistenti.
- Gli endpoint API di criteri consentono di eseguire il provisioning e gestire gli elenchi di destinazioni e le destinazioni per elenco.
- Gli endpoint API di report consentono di leggere e controllare in tempo reale le informazioni di protezione relative alle distribuzioni. L'API di individuazione applicazioni Umbrella fornisce informazioni dettagliate sulle applicazioni basate su cloud.

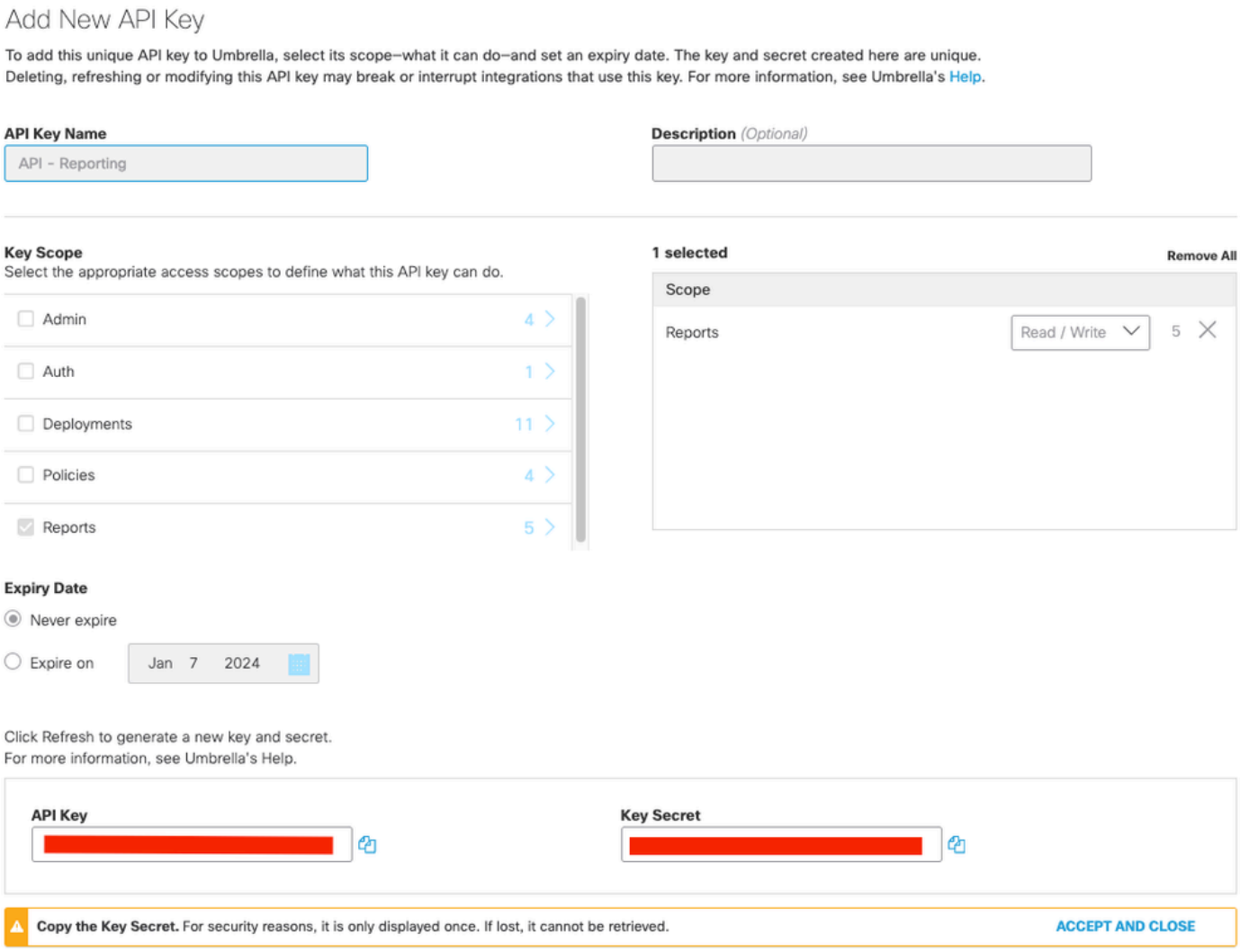
In questo articolo viene illustrato come raccogliere i report di ricerca delle attività tramite API.

Procedura Umbrella

1. Dal dashboard Umbrella, passare ad Amministrazione > Chiavi API.

2. Selezionare API Keys > Add.

3. In Ambito chiave, selezionare Report, quindi Crea chiave.



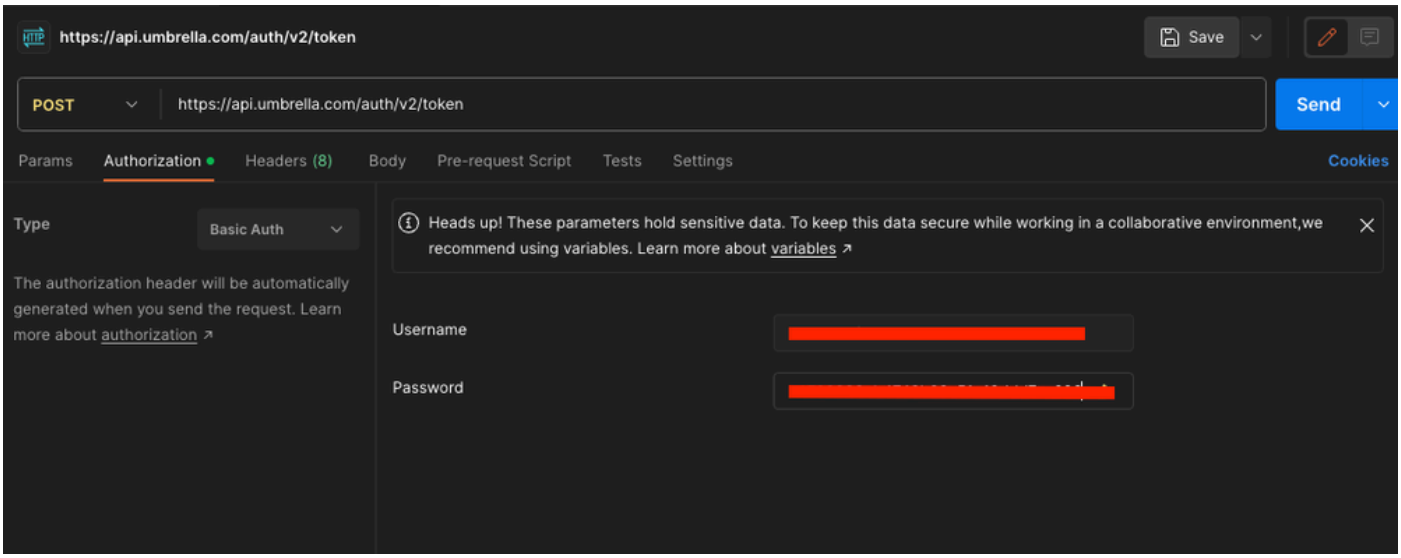
21495050167956

Gli amministratori possono regolare il livello di accesso per ambito tra lettura/scrittura e sola lettura, a seconda dell'uso previsto di ciascuna chiave API, mentre le chiavi API possono essere configurate per scadere in una data predefinita. In questa fase è necessario raccogliere la chiave/il segreto API, in quanto sono attualmente visibili e non possono essere visualizzati in seguito.

Le credenziali API generano token di accesso API validi per 60 minuti. Questa procedura supporta il flusso di credenziali del client OAuth 2.0. Negli ambienti Umbrella per più organizzazioni o provider di servizi, è possibile utilizzare le credenziali API dell'organizzazione padre per generare token di accesso con gli stessi ambiti per un'organizzazione figlio specificati durante il processo di autorizzazione.

Routine Postman

Innanzitutto, è necessario creare un token di accesso OAuth 2.0. I percorsi di autenticazione dell'API Umbrella iniziano con https://api.umbrella.com/auth/v2. Dopo l'invio di una query POST e di una chiave API utente come nome utente e password API come password, viene generato un token di accesso.

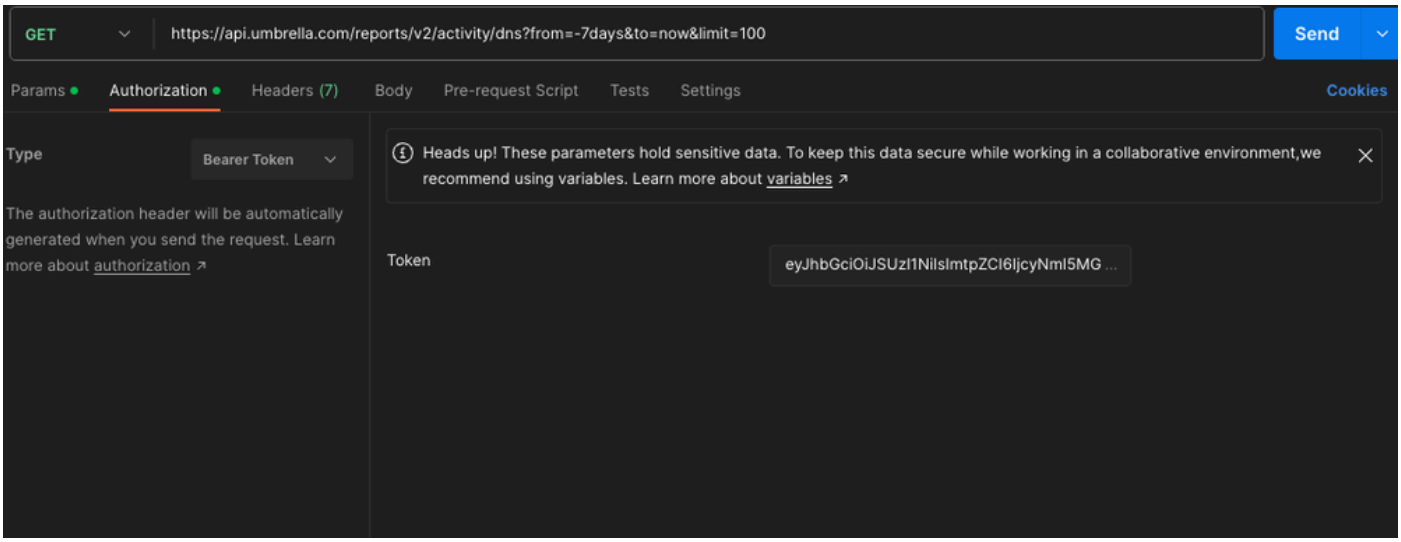


21606708808468

21607051456276

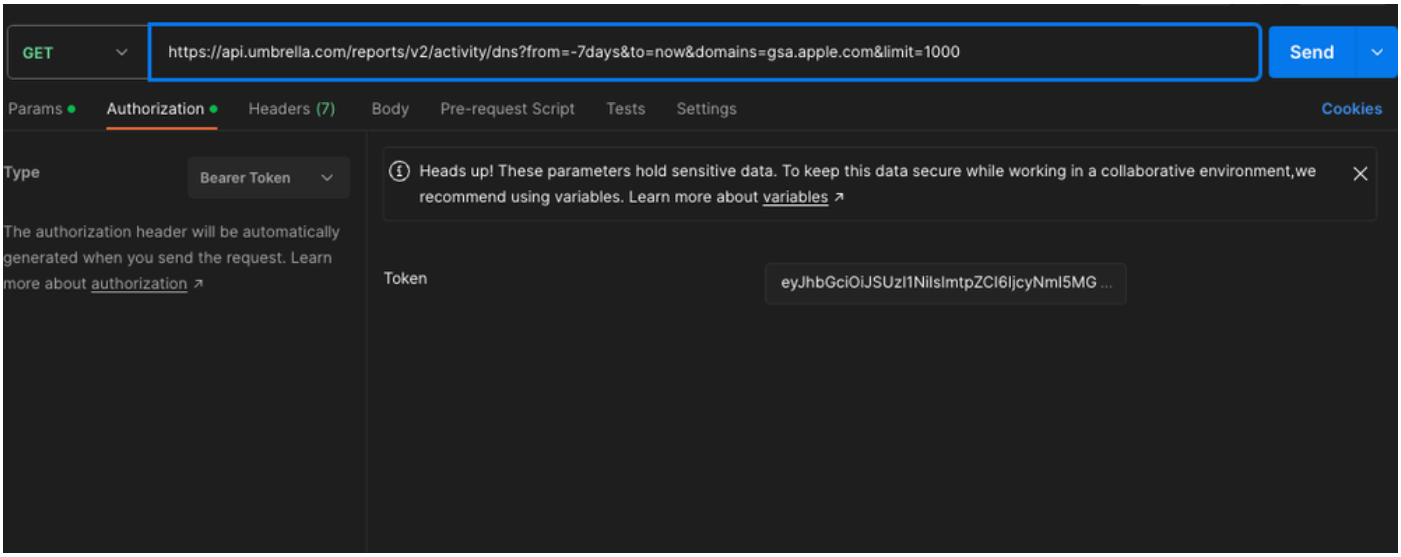
In questa fase, è necessario raccogliere il token di accesso. A questo punto è possibile recuperare le informazioni con il token di accesso.

È necessario selezionare il metodo GET e immettere sia il percorso API (incluso il parametro richiesto) che il token di accesso. In questo esempio è possibile recuperare 100 report dalla ricerca di attività esclusivamente per il traffico DNS degli ultimi 7 giorni.



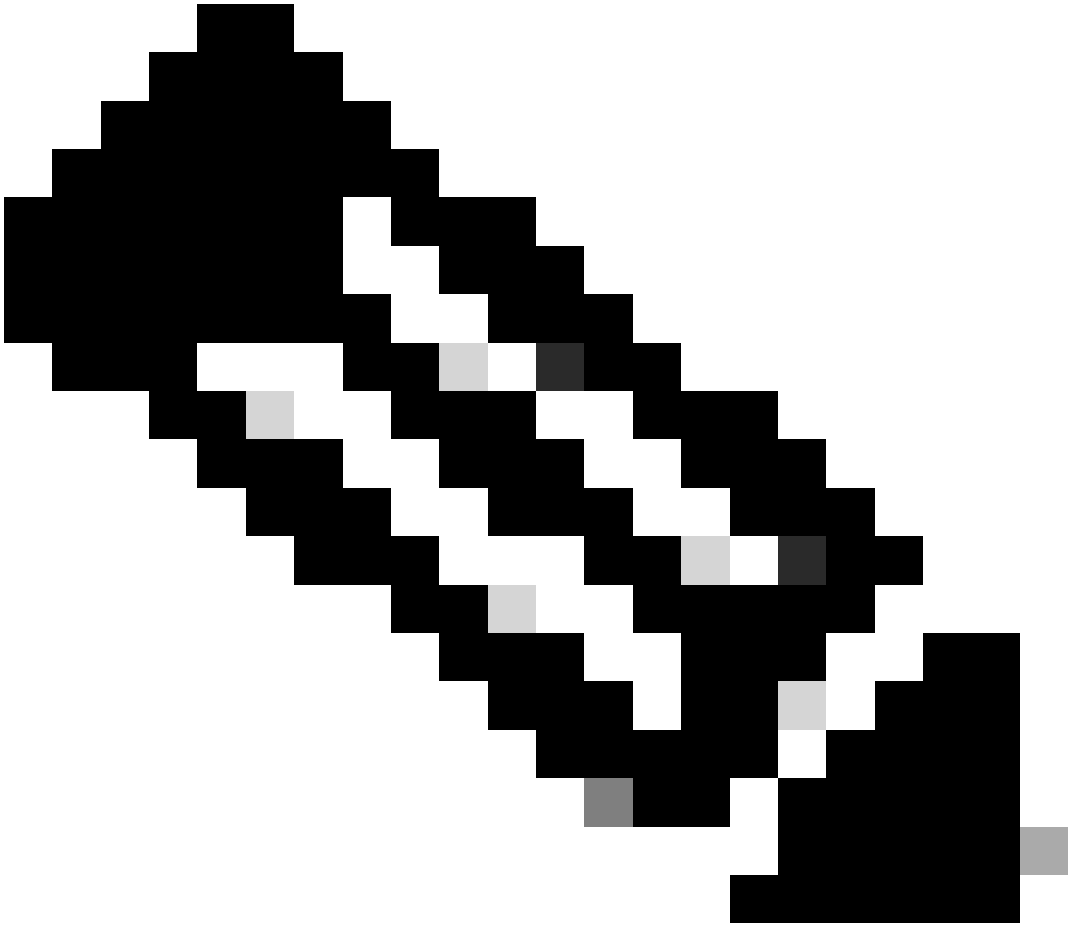
21607952074772

In un altro esempio, è possibile tentare di estrarre 1000 report dalla ricerca di attività, esclusivamente per il traffico DNS degli ultimi 7 giorni, in particolare per il dominio "gsa.apple.com".



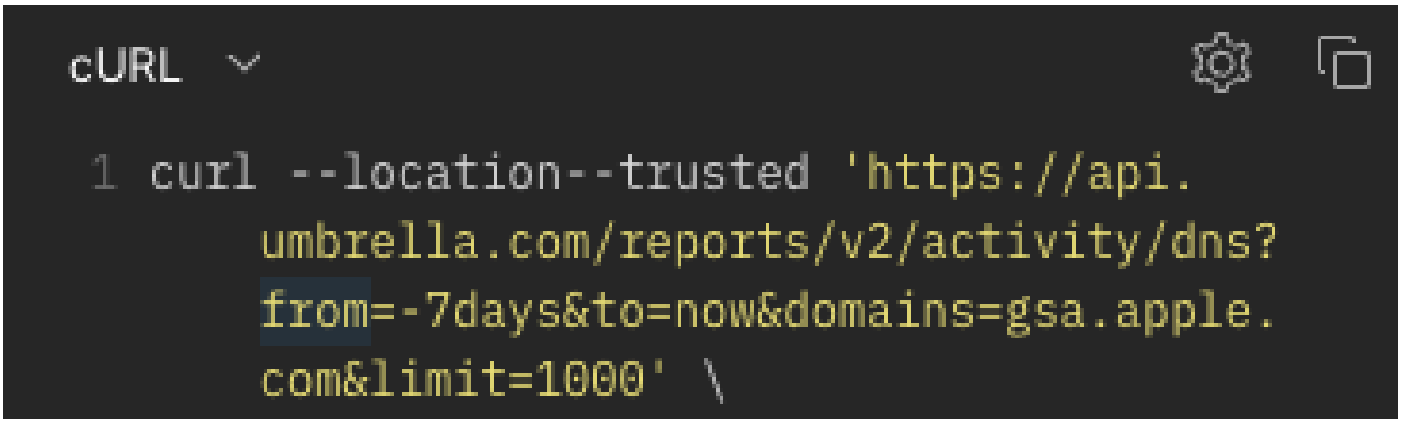
21607927544468

È possibile consultare Parametri query di richiesta per individuare ulteriori parametri che è possibile utilizzare nella query API.



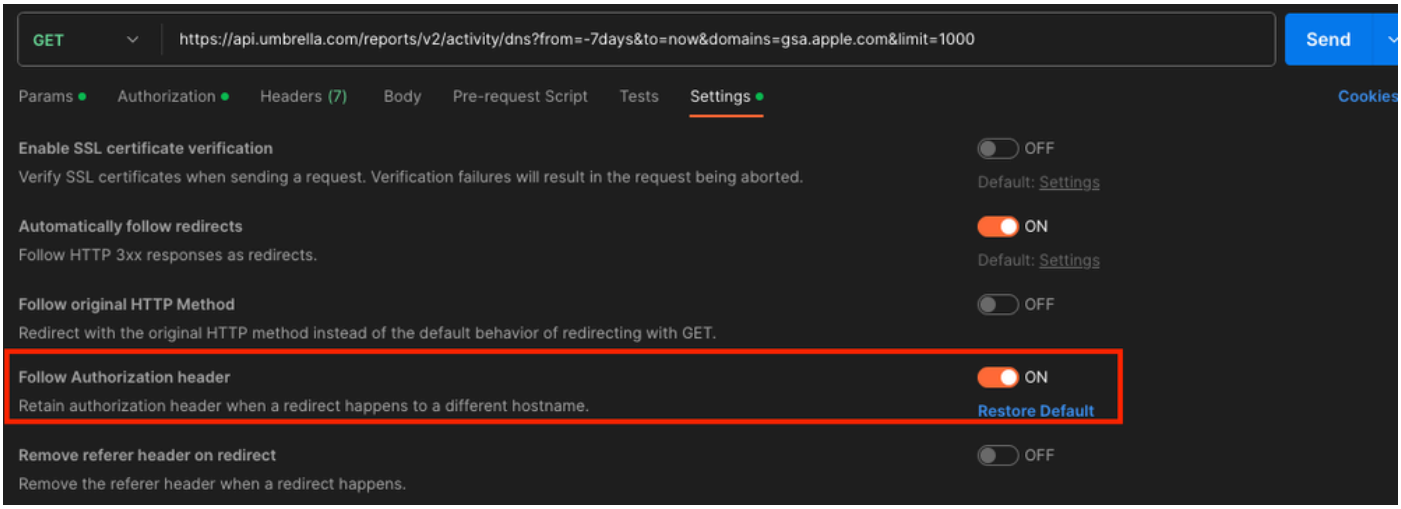
Nota: Se una richiesta client HTTP non proviene dallo stesso continente in cui si trova il data warehouse Umbrella, il server Umbrella risponde con 302 Trovato. Per reindirizzare automaticamente le richieste HTTP e mantenere l'intestazione dell'autorizzazione HTTP, è possibile impostare flag aggiuntivi o abilitare un'impostazione di reindirizzamento.

ricciolo: Per reindirizzare la richiesta HTTP corrente e mantenere l'intestazione Authorization, è necessario passare i flag -L o —location e —location-trusted.



21608126036628

Postino: Nell'ambiente Postman, passare a un'API e selezionare un metodo GET. Passare a Impostazioni > Abilita intestazione Segui autorizzazione per mantenere l'intestazione Autorizzazione per le richieste di reindirizzamento.



21608126042388

Risposte

Dopo aver inviato l'azione GET all'URL, è possibile ricevere vari codici di stato:

- Stato:200: Le informazioni richieste sono state accettate.
- Stato: 400: richiesta non valida. Può essere correlato all'URL inviato per la query. Uno o più parametri non sono corretti.
- Stato: 401: Non autorizzato. Intestazione dell'autorizzazione mancante o token non autorizzato.
- Stato:403: Non consentito. Token non valido.

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).