Configura DNS su HTTPS (DoH) con Umbrella

Sommario

Introduzione

In questo documento viene descritto come Umbrella supporta il DNS su HTTPS (DoH), crittografando le query DNS per la privacy.

Panoramica

Cisco Umbrella supporta il DNS su HTTPS (DoH), consentendo la crittografia e la protezione delle query DNS da intercettazioni o modifiche. Usa questo endpoint DoH:

Nome host	Descrizione
doh.umbrella.com	Frontend per il servizio DNS standard di Umbrella (208.67.222.222/220.220)

I passaggi per l'utilizzo di DoH con Umbrella dipendono dal browser e dal sistema operativo.

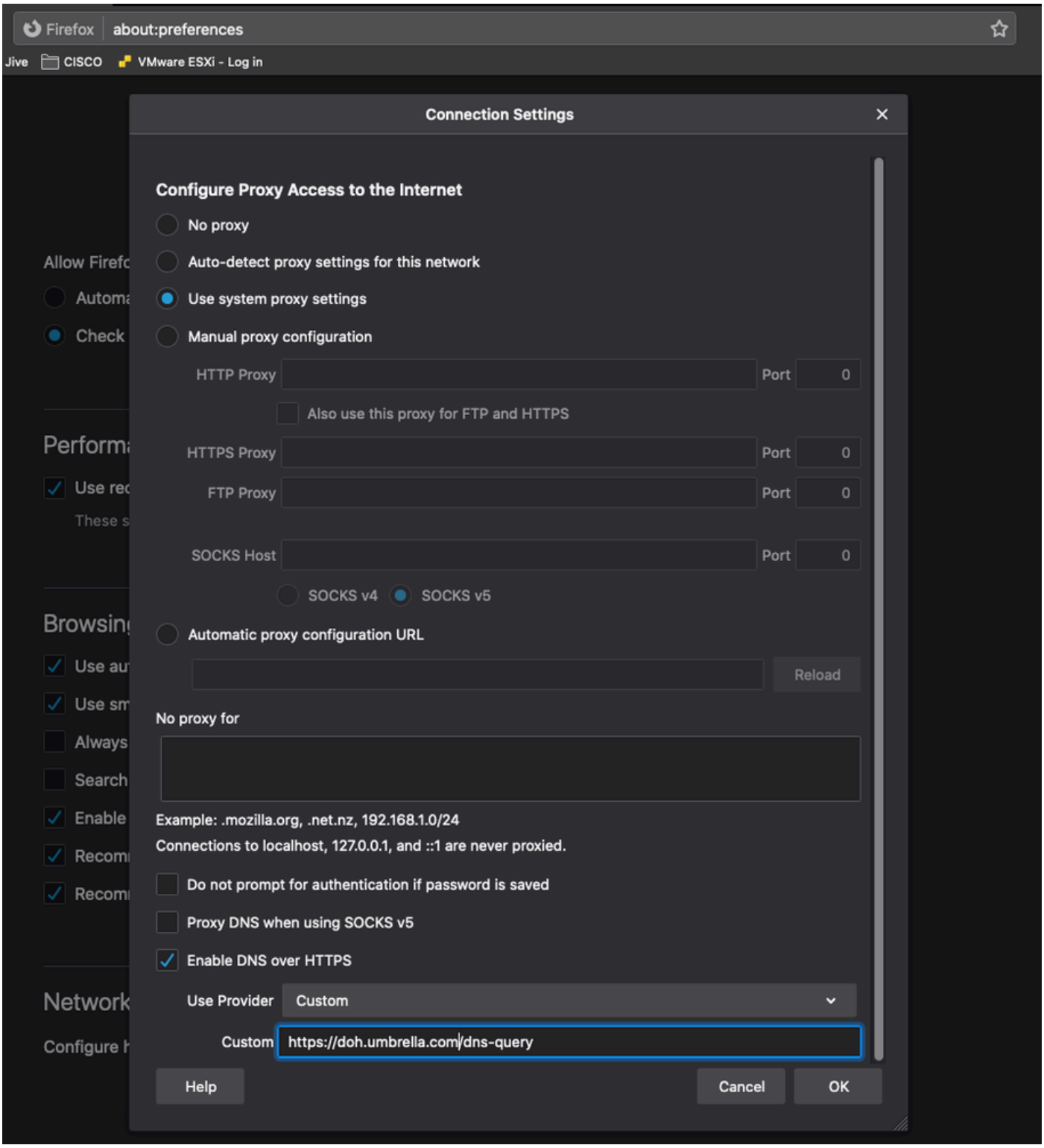
Mozilla Firefox

Dettagli e istruzioni sono disponibili su Mozilla. Firefox può essere configurato per utilizzare Umbrella come provider DNS personalizzato su HTTPS.

1. Selezionare Opzioni > Generale > Impostazioni di rete e selezionare Abilita DNS su HTTPS.
2. In Usa provider, scegliere Personalizzato e immettere il modello URI:
3.

```
https://umbrella.cisco.com/doh-help
```

4. Selezionare OK per crittografare le query.



Preferenze.png

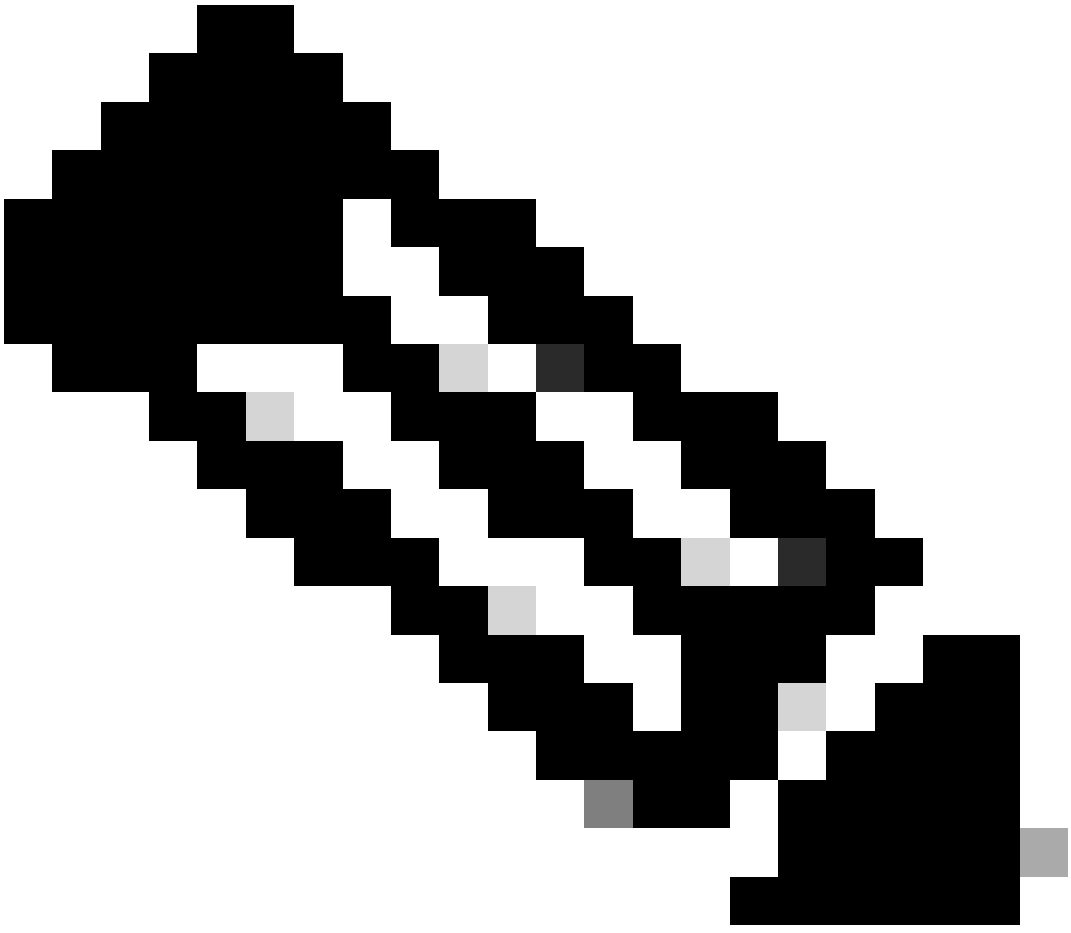
Google Chrome

Dettagli e istruzioni sulla configurazione sono disponibili sul Chromium Blog. Chrome abilita automaticamente l'uso di DoH se il DNS sicuro è abilitato e vede Umbrella indirizzi IP anycast utilizzati dal sistema operativo per DNS.

Configurare il sistema operativo in modo che utilizzi questi indirizzi IP come server DNS:

Servizio	Indirizzi IPv4	Indirizzi IPv6
Umbrella DNS	208.67.222.222 208.67.220.220	2620:119:35::35 2620:119:53::53

1. Nelle impostazioni di Chrome, passare a Privacy and security >Security (o immettere chrome://settings/security nella barra degli indirizzi).
2. Abilitare Usa DNS sicuro.
3. Le query DNS sono ora crittografate. È possibile visitare la pagina di prova Umbrella DoH per verificare la configurazione.



Nota: Chrome cerca gli indirizzi IP Umbrella in modo specifico quando si decide se eseguire l'aggiornamento a DoH. Ciò significa che se si è configurati per utilizzare

---

l'indirizzo IP di un server DNS o di un server d'inoltro locale, Chrome non può eseguire l'aggiornamento a utilizzando DoH, anche se quel server inoltra a Umbrella.

Se il computer è considerato gestito da Chrome, probabilmente se il computer viene fornito dall'azienda o dall'istituto di istruzione, non può eseguire l'aggiornamento automatico a utilizzando DoH, e questa impostazione non può essere visibile o configurabile.

Anziché eseguire l'aggiornamento automatico in base all'indirizzo IP, è possibile configurare Umbrella direttamente impostando un provider personalizzato. In Usa DNS sicuro, selezionare Con, quindi scegliere Personalizzato dall'elenco a discesa. Se viene richiesto di immettere un provider personalizzato, aggiungere il modello Umbrella URI nel formato seguente:

```
https://doh.umbrella.com/dns-query
```

Avvertenze

In alcune situazioni, è possibile che si verifichi un conflitto tra il DoH e il SWG di Umbrella (in particolare il modulo AnyConnect):

1. La funzionalità relativa ai domini esterni di AnyConnect consente ai domini e agli indirizzi IP di ignorare Umbrella SWG passando direttamente a Internet. Quando si utilizza DoH, non è possibile configurarlo in base al nome di dominio o al nome di dominio qualificato di frequente (FQDN). AnyConnect infatti si basa sulla cache DNS del sistema operativo per collegare i nomi di dominio agli indirizzi IP e rilevare le richieste che passano al protocollo SWG e le ignorano. Quando DOH viene utilizzato (in particolare da un browser), il resolver di stub DNS per il sistema operativo viene ignorato e di conseguenza non viene creata alcuna voce della cache DNS. In questo modo AnyConnect non è in grado di correlare un nome di dominio o un FQDN da ignorare al pacchetto che sta visualizzando.

   ### Soluzioni

   Disabilitare DOH sulle workstation che usano AnyConnect per Umbrella SWG e/o configurare i domini esterni (eccezioni SWG) con l'indirizzo IP anziché con il dominio o il nome di dominio completo.

2. Se il protocollo DoH viene usato per la risoluzione delle risorse interne (ad esempio.local o example.corp) da un server DNS interno, il protocollo AnyConnect Umbrella SWG deve essere configurato in modo da non intercettare le richieste DOH. Infatti, il DoH ha l'aspetto di qualsiasi altra richiesta HTTPS e il modulo SWG la intercetta e la reindirizza a Umbrella. Se

il server DoH non è accessibile dal cloud Umbrella, la query non raggiunge mai il server DNS interno destinato.

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).