# Umbrellaを使用したDNS over HTTPS(DoH)の設定

## 内容



## はじめに

このドキュメントでは、UmbrellaがDNS over HTTPS(DoH)をサポートし、プライバシーのためにDNSクエリを暗号化する方法について説明します。

## 概要

Cisco UmbrellaはDNS over HTTPS(DoH)をサポートしているため、DNSクエリを暗号化し、傍受や改ざんから保護できます。次のDoHエンドポイントを使用します。

| ホスト名 | 説明 |
| --- | --- |
| doh.umbrella.com | Umbrellaの標準DNSサービスのフロントエンド(208.67.222.222/220.220) |

DoHをUmbrellaで使用するための手順は、ブラウザとオペレーティングシステムによって異なります。

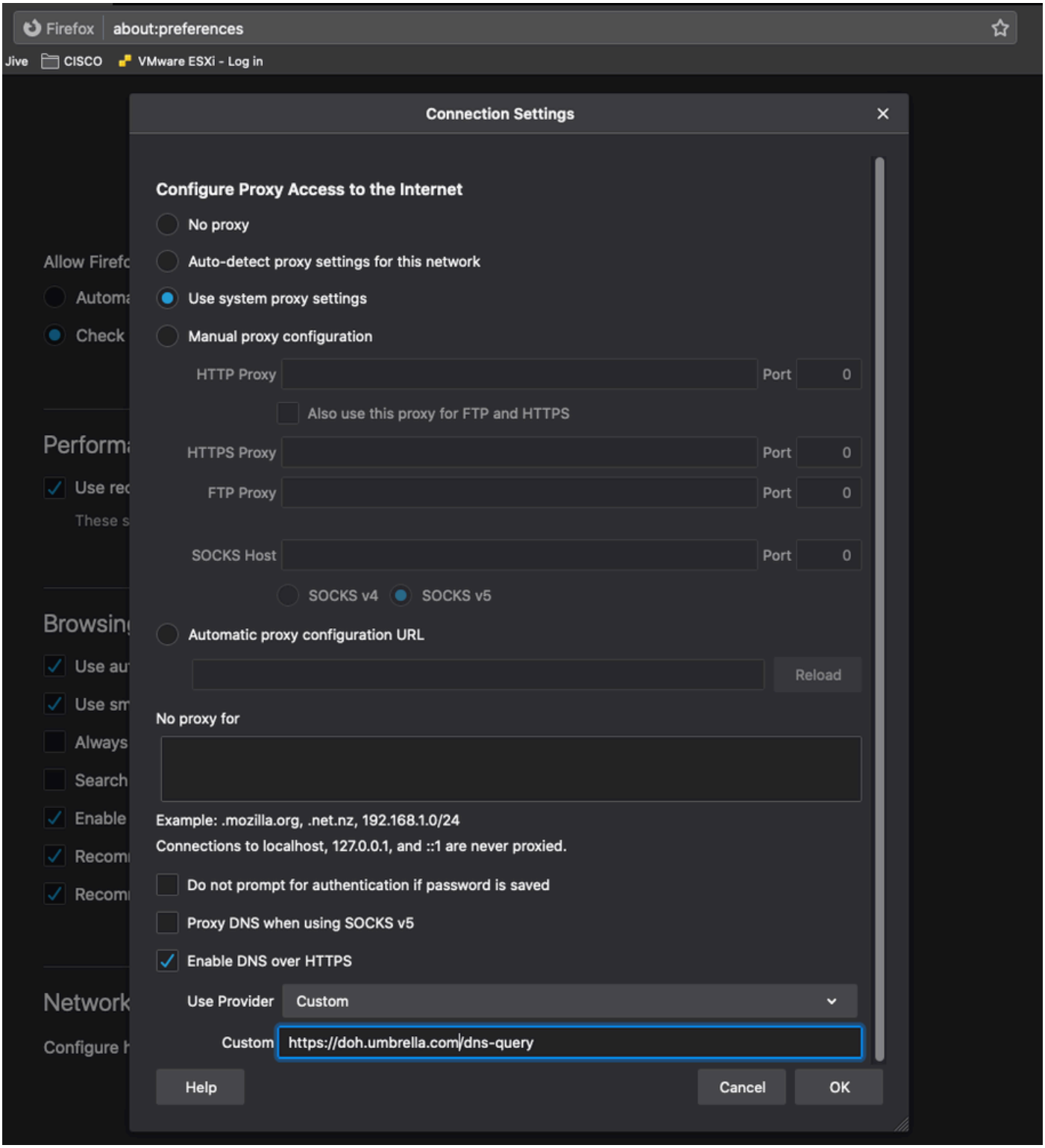
## Mozilla Firefox

詳細と手順はMozillaから入手できます。Firefoxは、カスタムDNS over HTTPSプロバイダーとしてUmbrellaを使用するように設定できます。

1. Options > General > Network Settingsの順に移動し、Enable DNS over HTTPSを選択します。
2. Use Providerの下で、Customを選択し、URI templateを入力します。
3. 

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

4. OKを選択すると、クエリが暗号化されます。




基本設定.png

## Google Chrome

設定の詳細と手順については、[Chromium Blog]を参照してください。Secure DNSが有効になって

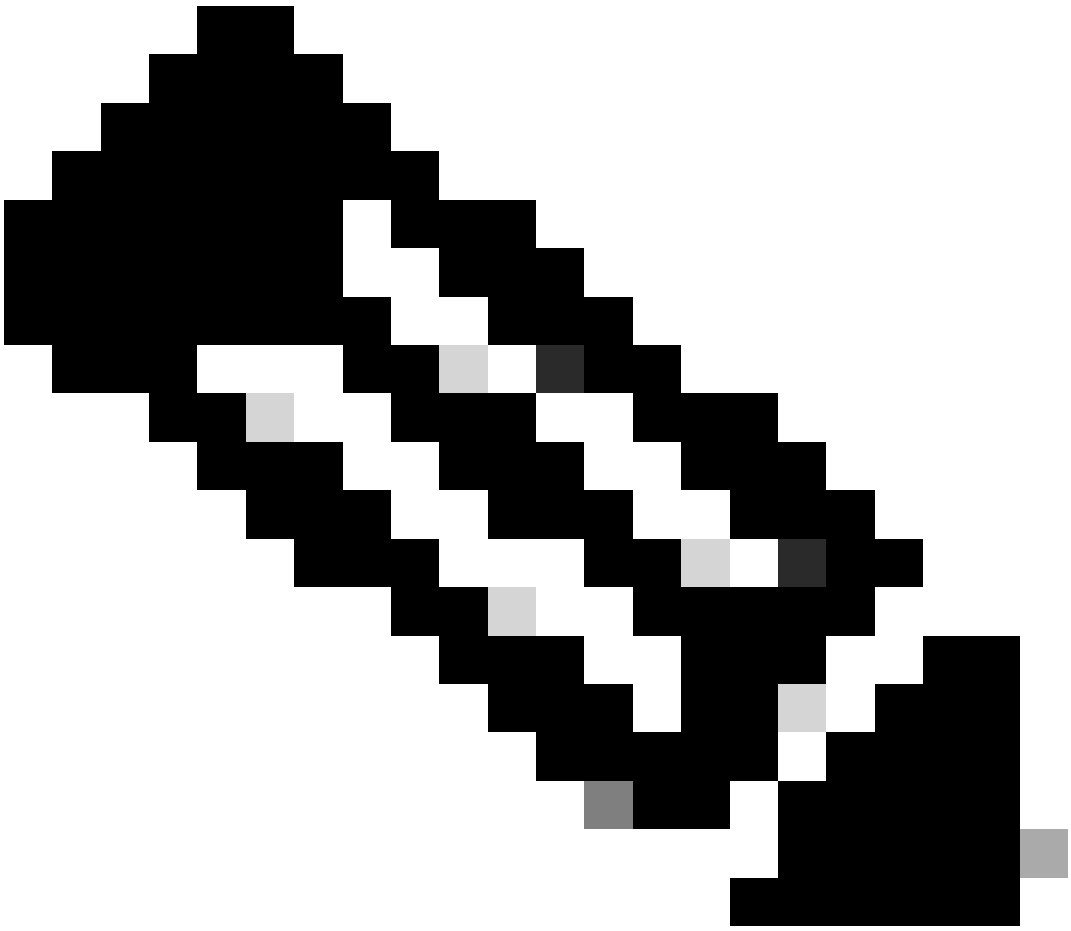
いて、オペレーティングシステムでDNSに使用されるUmbrellaエニーキャストIPアドレスが認識される場合、Chromeは自動的にDoHの使用を有効にします。

次のIPアドレスをDNSサーバとして使用するようにOSを設定します。

| サービス | IPv4アドレス | IPv6アドレス |
| --- | --- | --- |
| 包括DNS | 208.67.222.222<br>208.67.220.220 | 2620:119:35::35<br>2620:119:53::53 |

1. Chromeの設定で、Privacy and security >Security に移動します(またはアドレスバーにchrome://settings/securityと入力します)。
2. Use secure DNSを有効にします。
3. これで、DNSクエリが暗号化されました。Umbrella DoH Test Pageにアクセスして、設定を確認できます。

---



---

> 注:ChromeはDoHにアップグレードするかどうかを決定するときに、特にUmbrellaのIPアドレスを探します。つまり、ローカルDNSサーバまたはフォワーダのIPアドレスを使用するように設定されている場合、そのサーバがUmbrellaに転送されても、ChromeはDoHを使用してにアップグレードできません。

コンピュータがChromeによって管理されていると見なされる場合（職場または学校からコンピュータが提供されている場合）、DoHを使用するようにに自動アップグレードすることはできず、この設定を表示または構成することはできません。

IPに基づいて自動アップグレードを行う代わりに、カスタムプロバイダーを設定してUmbrellaを直接設定できます。Use secure DNSの下で、Withを選択し、ドロップダウンからCustomを選択します。カスタムプロバイダーの入力を求められる場所で、Umbrella URIテンプレートを次の形式で追加します。

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

## 警告

DoHとUmbrella SWG（特にAnyConnectモジュール）の間で競合が発生する可能性のある状況がいくつかあります。

1. AnyConnectの外部ドメイン機能を使用すると、インターネットに直接接続する代わりに、ドメインとIPアドレスでUmbrella SWGをバイパスできます。DoHを使用する場合、ドメイン名またはFQDN (Frequently Qualified Domain Name)で構成することはできません。これは、AnyConnectがSWGに送信される要求とSWGをバイパスする要求を検出する際に、ドメイン名をIPアドレスにリンクするためにオペレーティングシステムのDNSキャッシュに依存するためです。DOHが（特にブラウザによって）使用される場合、オペレーティングシステムのDNSスタブリゾルバはバイパスされ、その結果DNSキャッシュエントリは作成されません。そのため、AnyConnectはバイパスするドメイン名またはFQDNと検出したパケットを関連付けることができません。

   ### 回避策

   Umbrella SWG用にAnyConnectを使用してワークステーション上でDOHを無効にするか、またはドメインやFQDNの代わりにIPアドレスで外部ドメイン（SWG例外）を設定します。

2. 内部DNSサーバが内部リソース（example.localまたはexample.corpなど）の解決にDoHを使用する場合、これらのDOH要求を代行受信しないようにAnyConnect Umbrella SWGを設

定する必要があります。これは、DoHが他のHTTPS要求と同様に見え、SWGモジュールがそれをインターセプトしてUmbrellaにリダイレクトするためです。DoHサーバがUmbrellaクラウドからアクセスできない場合、クエリは宛先の内部DNSサーバに到達しません。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。