DNS über HTTPS (DoH) mit Umbrella konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Umbrella DNS über HTTPS (DoH) unterstützt und DNS-Abfragen verschlüsselt, um den Datenschutz zu gewährleisten.

Überblick

Cisco Umbrella unterstützt DNS over HTTPS (DoH), sodass DNS-Abfragen verschlüsselt und vor Abfangen oder Ändern geschützt werden können. Diesen DoH-Endpunkt verwenden:

Hostname	Beschreibung
doh.umbrella.com	Frontend für den Standard-DNS-Dienst von Umbrella (208.67.222.222/220.220)

Die Vorgehensweise bei der Verwendung von DoH mit Umbrella hängt von Ihrem Browser und Betriebssystem ab.

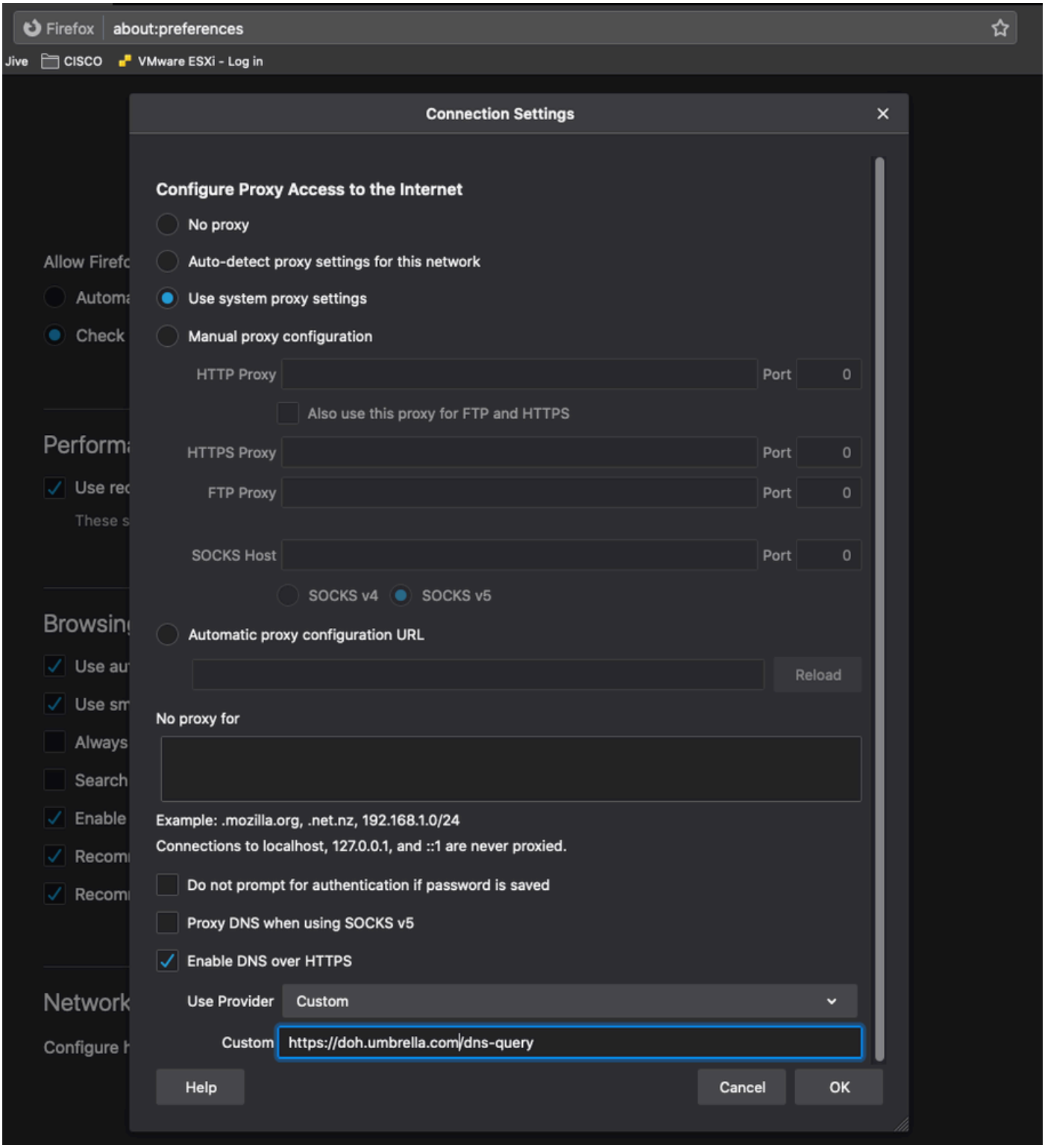
Mozilla Firefox

Details und Anleitungen erhalten Sie von Mozilla. Firefox kann so konfiguriert werden, dass Umbrella als benutzerdefinierter DNS über HTTPS-Provider verwendet wird.

1. Navigieren Sie zu Optionen > Allgemein > Netzwerkeinstellungen, und wählen Sie DNS über HTTPS aktivieren aus.
2. Wählen Sie unter Provider verwenden die Option Benutzerdefiniert aus, und geben Sie die URI-Vorlage ein:
3.

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

4. Wählen Sie OK, und Ihre Abfragen werden verschlüsselt.



Preferences.png

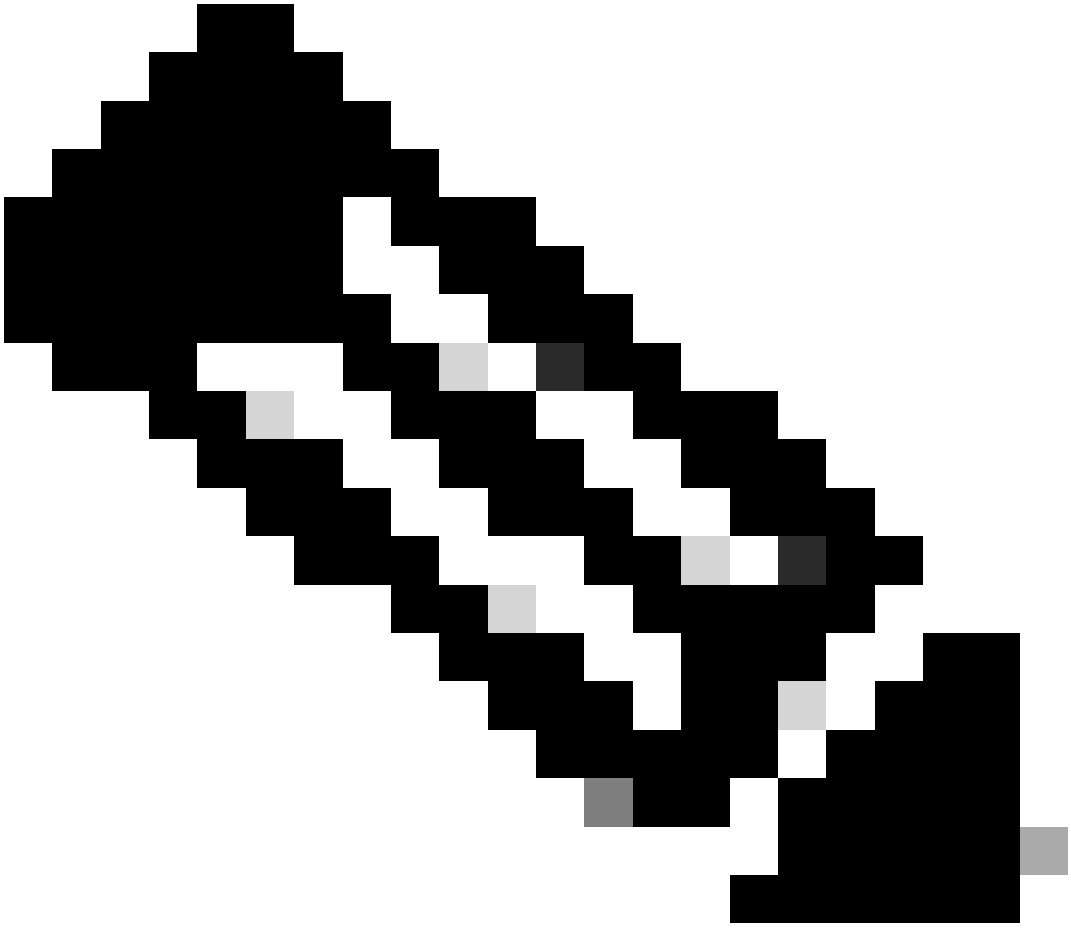
Google Chrome

Details und Anleitungen zur Konfiguration finden Sie im Chrom-Blog. Chrome aktiviert automatisch die Verwendung von DoH, wenn Secure DNS aktiviert ist, und erkennt Umbrella Anycast IP-Adressen vom Betriebssystem für DNS verwendet.

Konfigurieren Sie Ihr Betriebssystem zur Verwendung dieser IP-Adressen als DNS-Server:

Service	IPv4-Adressen	IPv6-Adressen
Umbrella DNS	208.67.222.222 208.67.220.220	2620:119:35::35 2620:119:53::53

1. Navigieren Sie in den Chrome-Einstellungen zu Datenschutz und Sicherheit > Sicherheit (Oder geben Sie chrome://settings/security in die Adressleiste ein).
2. Aktivieren Sie Sicheren DNS verwenden.
3. Ihre DNS-Abfragen sind jetzt verschlüsselt. Sie können die Umbrella DoH-Testseite besuchen, um Ihre Konfiguration zu überprüfen.



> Anmerkung: Chrome sucht die Umbrella IP-Adressen speziell bei der Entscheidung, ob ein Upgrade auf DoH. Das bedeutet, dass Chrome, wenn Sie für die Verwendung der IP-Adresse eines lokalen DNS-Servers oder -Forwarders konfiguriert sind, kein Upgrade auf DoH durchführen kann, selbst wenn dieser Server an Umbrella weiterleitet.

Wenn Ihr Computer als von Chrome verwaltet gilt, was wahrscheinlich ist, wenn Ihr Computer von Ihrer Arbeit oder Schule bereitgestellt wird, kann er nicht automatisch auf DoH aktualisiert werden, und diese Einstellung kann nicht sichtbar oder konfigurierbar sein.

Anstatt ein automatisches IP-basiertes Upgrade durchzuführen, können Sie Umbrella direkt konfigurieren, indem Sie einen benutzerdefinierten Anbieter festlegen. Wählen Sie unter Sicheren DNS verwenden die Option Mit aus, und wählen Sie im Dropdown-Menü die Option Benutzerdefiniert aus. Wenn Sie aufgefordert werden, einen benutzerdefinierten Anbieter einzugeben, fügen Sie die Umbrella URI-Vorlage in folgendem Format hinzu:

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

Hinweise

Es gibt Situationen, die einen Konflikt zwischen DoH und Umbrella SWG verursachen können (insbesondere das AnyConnect-Modul):

1. Die Funktion für externe Domänen in AnyConnect ermöglicht es Domänen und IP-Adressen, die Umbrella SWG zu umgehen, indem sie stattdessen direkt ins Internet gehen. Bei Verwendung von DoH kann die Domäne nicht nach Domänenname oder nach FQDN (Frequently Qualified Domain Name) konfiguriert werden. Dies liegt daran, dass AnyConnect auf den DNS-Cache im Betriebssystem angewiesen ist, um Domänennamen mit IP-Adressen zu verknüpfen, wenn erkannt wird, welche Anfragen an die SWG gehen und welche diese umgehen. Wenn DOH verwendet wird (insbesondere von einem Browser), wird der DNS-Stub-Resolver für das Betriebssystem umgangen und folglich kein DNS-Cache-Eintrag erstellt. Daher kann AnyConnect einen zu umgehenden Domänennamen oder FQDN nicht mit dem Paket korrelieren, das er sieht.

   ## Problemumgehungen

   Deaktivieren Sie DOH auf Workstations, die AnyConnect für Umbrella SWG verwenden, und/oder konfigurieren Sie externe Domänen (SWG-Ausnahmen) nach IP-Adresse anstatt nach Domäne oder FQDN.

2. Wenn DoH für die Auflösung interner Ressourcen (z. B. example.local oder example.corp) durch einen internen DNS-Server verwendet wird, muss die AnyConnect Umbrella SWG so konfiguriert werden, dass diese DOH-Anforderungen nicht abgefangen werden. Der Grund hierfür ist, dass DoH wie jede andere HTTPS-Anforderung aussieht und vom SWG-Modul abgefangen und an Umbrella umgeleitet wird. Wenn der DoH-Server nicht von der Umbrella-Cloud aus erreichbar ist, erreicht die Abfrage niemals den internen DNS-Zielserver.

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.