

DNS configureren via HTTPS (DoH) met paraplu

Inhoud

[Inleiding](#)

[Overzicht](#)

[Mozilla Firefox](#)

[Google Chrome](#)

[Voorbehouden](#)

[tijdelijke oplossingen](#)

Inleiding

In dit document wordt beschreven hoe Umbrella DNS over HTTPS (DoH) ondersteunt, waarbij DNS-zoekopdrachten voor privacy worden gecodeerd.

Overzicht

Cisco Umbrella ondersteunt DNS over HTTPS (DoH), waardoor DNS-query's kunnen worden gecodeerd en beschermd tegen onderschepping of wijziging. Gebruik dit DoH-eindpunt:

Hostnaam	Beschrijving
doh.umbrella.com	Frontend voor de standaard DNS-service van Umbrella (208.67.222.222/220.220)

Stappen voor het gebruik van DoH met Umbrella zijn afhankelijk van uw browser en besturingssysteem.

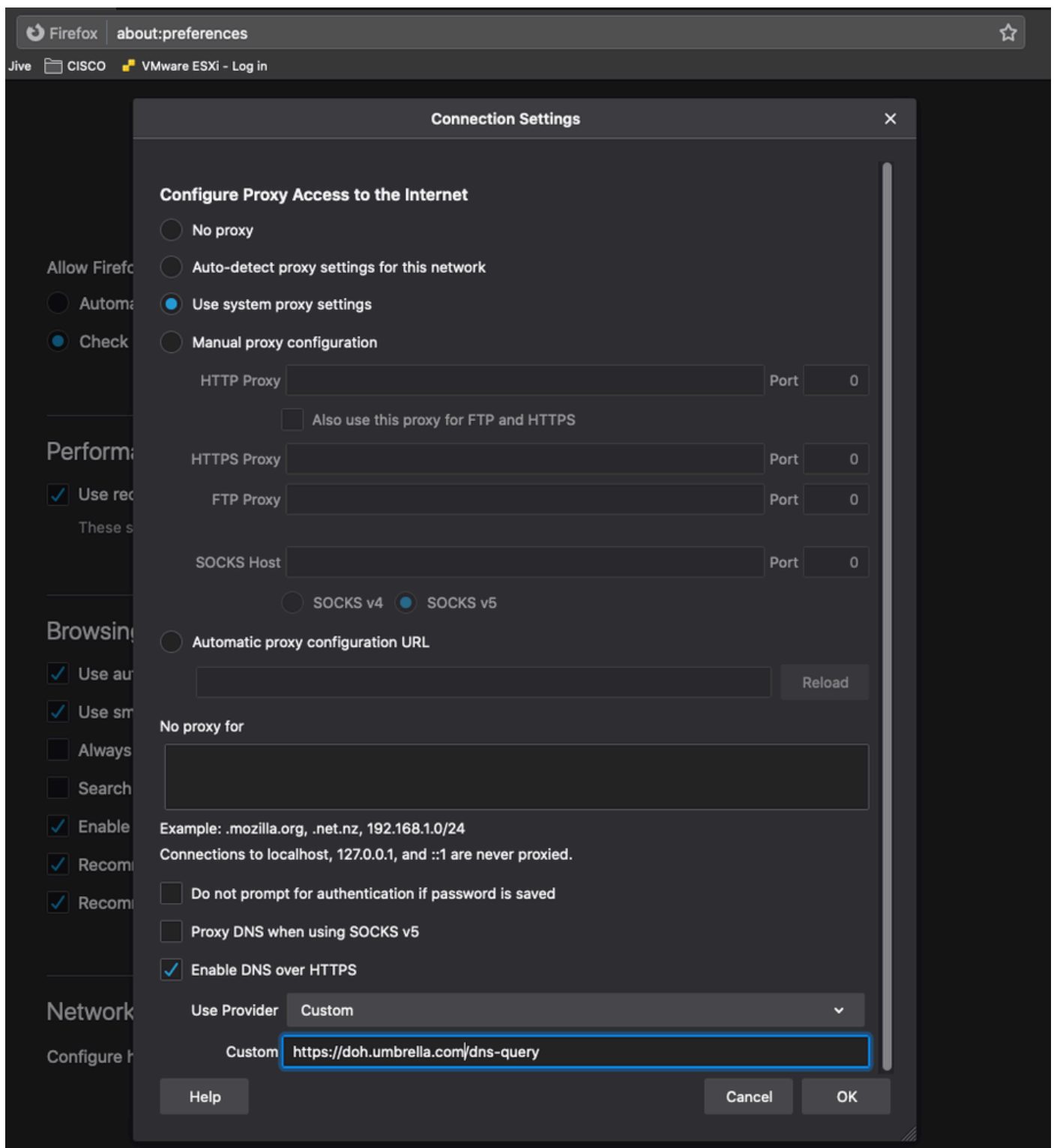
Mozilla Firefox

Details en instructies zijn beschikbaar bij [Mozilla](#). Firefox kan worden geconfigureerd om Umbrella te gebruiken als een aangepaste DNS over HTTPS-provider.

1. Navigeer naar Opties > Algemeen > Netwerkinstellingen en selecteer DNS inschakelen via HTTPS.
2. Kies onder Provider gebruiken de optie Aangepast en voer de URI-sjabloon in:
- 3.

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

4. Selecteer OK en uw zoekopdrachten zijn gecodeerd.



Voorkeuren.png

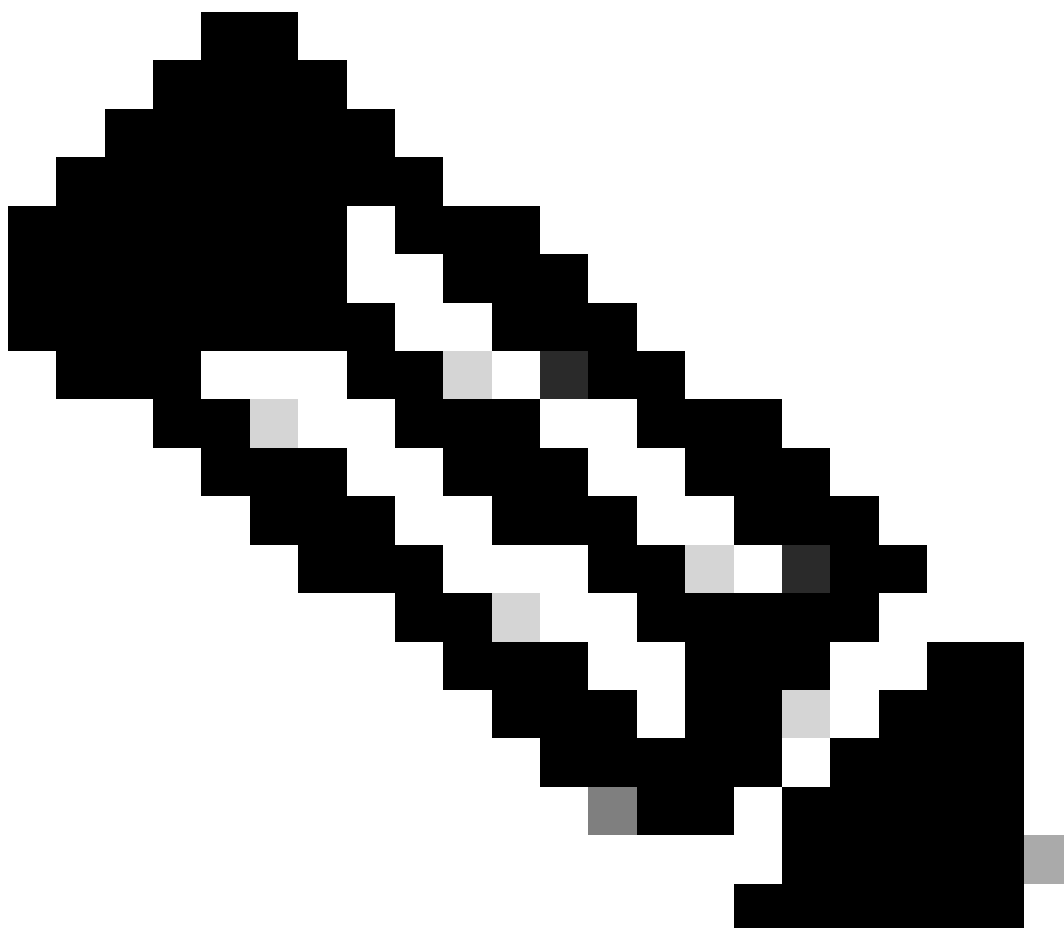
Google Chrome

Details en instructies over de configuratie zijn beschikbaar op de [Chromium Blog](#). Chrome schakelt automatisch het gebruik van DoH in als Secure DNS is ingeschakeld en het ziet Umbrella anycast IP-adressen die worden gebruikt door het besturingssysteem voor DNS.

Configureer uw besturingssysteem om deze IP-adressen als DNS-servers te gebruiken:

dienst	IPv4-adressen	IPv6-adressen
Umbrella DNS	208.67.222.222	2620:119:35::35
	208.67.220.220	2620:119:53::53

1. Navigeer in de Chrome-instellingen naar Privacy en beveiliging > Beveiliging (Of voer chrome://settings/security in de adresbalk in).
 2. Maak gebruik van beveiligde DNS.
 3. Uw DNS-query's zijn nu gecodeerd. U kunt de [Umbrella DoH-testpagina](#) bezoeken om uw configuratie te controleren.
-



Opmerking: Chrome zoekt specifiek naar de IP-adressen van Umbrella wanneer wordt besloten om te upgraden naar DoH. Dit betekent dat als u bent geconfigureerd voor het

gebruik van het IP-adres van een lokale DNS-server of forwarder, Chrome niet kan upgraden naar het gebruik van DoH, zelfs als die server doorstuurt naar Umbrella.

Als uw computer wordt beschouwd als beheerd door Chrome, wat waarschijnlijk is als uw computer door uw werk of school aan u wordt verstrekt, [kan deze niet automatisch worden bijgewerkt naar het gebruik van DoH](#), en deze instelling kan niet zichtbaar of configureerbaar zijn.

In plaats van automatisch upgraden op basis van IP, kunt u Umbrella rechtstreeks configureren door een aangepaste provider in te stellen. Selecteer onder Gebruik beveiligde DNS de optie Met en kies Aangepast in de vervolgkeuzelijst. Waar het vraagt om een aangepaste provider in te voeren, voegt u de overkoepelende URI-sjabloon in dit formaat toe:

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

Voorbehouden

Er zijn enkele situaties die u kunt tegenkomen die een conflict veroorzaken tussen DoH en Umbrella SWG (met name de AnyConnect-module):

1. Met de functie Externe domeinen in AnyConnect kunnen domeinen en IP-adressen Umbrella SWG omzeilen door in plaats daarvan rechtstreeks naar internet te gaan. Het kan niet worden geconfigureerd op domeinnaam of Frequently Qualified Domain Name (FQDN) bij het gebruik van DoH. Dit komt omdat AnyConnect vertrouwt op de DNS-cache in het besturingssysteem om domeinnamen te koppelen aan IP-adressen bij het detecteren welke verzoeken naar SWG gaan en welke deze omzeilt. Wanneer DOH wordt gebruikt (vooral door een browser), wordt de DNS-stub-resolver voor het besturingssysteem omzeild en wordt er bijgevolg geen DNS-cachevermelding gemaakt. Dit laat AnyConnect niet in staat om een domeinnaam of FQDN te correleren om te omzeilen, met het pakket dat het ziet.

tijdelijke oplossingen

Schakel DOH uit op werkstations met AnyConnect for Umbrella SWG en/of configureer External Domains (SWG-uitzonderingen) op basis van IP-adres in plaats van op basis van domein of FQDN.

2. Als DoH wordt gebruikt voor het oplossen van interne bronnen (zoals example.local of example.corp) door een interne DNS-server, moet AnyConnect Umbrella SWG worden geconfigureerd om deze DOH-verzoeken niet te onderscheppen. Dit komt omdat DoH eruit ziet als elk ander HTTPS-verzoek en de SWG-module het onderschept en doorstuurt naar

Umbrella. Als de DoH-server niet toegankelijk is vanuit de Umbrella-cloud, bereikt de query nooit de beoogde interne DNS-server.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.