Configure DNS over HTTPS (DoH) with Umbrella

Contents

Introduction

This document describes how Umbrella supports DNS over HTTPS (DoH), encrypting DNS queries for privacy.

Overview

Cisco Umbrella supports DNS over HTTPS (DoH), allowing DNS queries to be encrypted and protected from interception or modification. Use this DoH endpoint:

Hostname	**Description**
doh.umbrella.com	Frontend for Umbrella's standard DNS service (208.67.222.222/220.220)

Steps for using DoH with Umbrella depend on your browser and operating system.

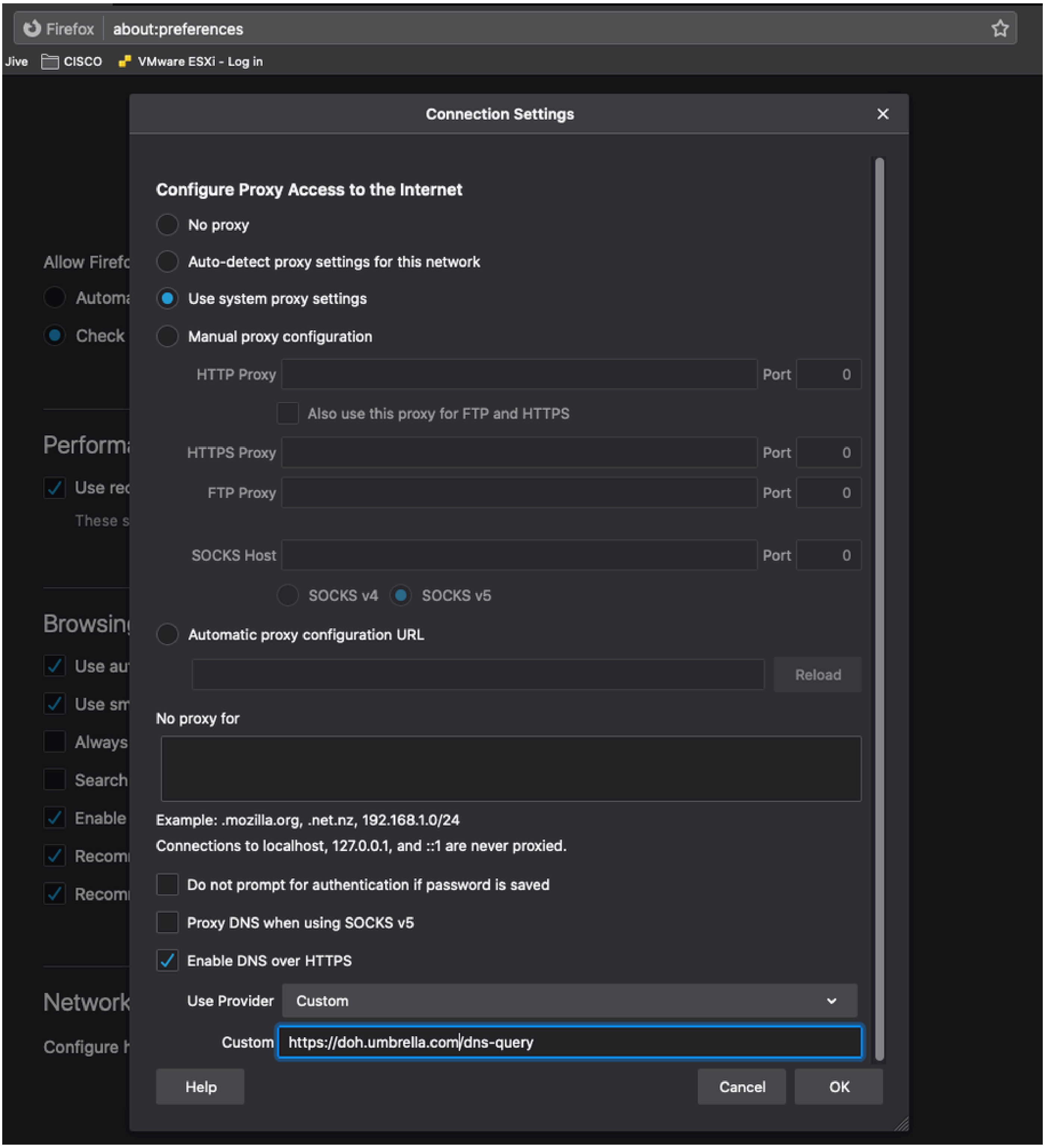
Mozilla Firefox

Details and instructions are available from Mozilla. Firefox can be configured to use Umbrella as a custom DNS over HTTPS provider.

1. Navigate to **Options** > **General** > **Network Settings** and select **Enable DNS over HTTPS**.
2. Under **Use Provider**, choose **Custom** and enter the **URI template**:
3.

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

4. Select **OK** and your queries are encrypted.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

● Use system proxy settings

○ Manual proxy configuration

HTTP Proxy Port 0

□ Also use this proxy for FTP and HTTPS

HTTPS Proxy Port 0

FTP Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved

□ Proxy DNS when using SOCKS v5

☑ Enable DNS over HTTPS

Use Provider: Custom

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

Preferences.png

Google Chrome

Details and instructions on configuration are available from the Chromium Blog. Chrome automatically enables the use of DoH if Secure DNS is enabled and it sees Umbrella anycast IP addresses used by the operating system for DNS.

Configure your OS to use these IP addresses as DNS servers:

Service	**IPv4 Addresses**	**IPv6 Adresses**
Umbrella DNS	208.67.222.222 208.67.220.220	2620:119:35::35 2620:119:53::53

1. In the Chrome settings, navigate to **Privacy and security >Security** (Or enter **chrome://settings/security** into the address bar).
2. Enable **Use secure DNS**.
3. Your DNS queries are now encrypted. You can visit the Umbrella DoH Test Page to check your configuration.

Note: Chrome looks for the Umbrella IP addresses specifically when deciding whether to upgrade to DoH. This means if you are configured to use the IP address of a local DNS server or forwarder, Chrome cannot upgrade to using DoH, even if that server forwards to Umbrella.

If your computer is considered managed by Chrome, which is likely if your computer is provided to you by your work or school, it cannot auto-upgrade to using DoH, and this setting cannot be visible or configurable.

Instead of auto-upgrading based on IP, you can configure Umbrella directly by setting a custom provider. Under **Use secure DNS**, select **With** and choose **Custom** from the drop-down. Where it asks to enter custom provider, add the **Umbrella URI template** in this format:

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

Caveats

There are some situations you can encounter that cause a conflict between DoH and Umbrella SWG (notably the AnyConnect module):

1. The External Domains feature in AnyConnect allows domains and IP addresses to bypass Umbrella SWG by going direct to the internet instead. It cannot be configured by domain name, or Frequently Qualified Domain Name (FQDN), when using DoH. This is because AnyConnect relies on the DNS cache in the operating system to link domain names to IP addresses when detecting which requests go to SWG and which bypasses it. When DOH is utilized (especially by a browser), the DNS stub resolver for the operating system is bypassed and consequently no DNS cache entry is created. This leaves AnyConnect unable to correlate a domain name or FQDN to bypass, with the packet it is seeing.

   ### Workarounds

   Disable DOH on workstations using AnyConnect for Umbrella SWG, and/or configure External Domains (SWG exceptions) by IP address instead of domain or FQDN.

2. If DoH is used for resolution of internal resources (such as example.local or example.corp) by an internal DNS server, AnyConnect Umbrella SWG must be configured to not intercept those DOH requests. This is because DoH looks like any other HTTPS request, and the SWG module intercepts it and redirects it to Umbrella. If the DoH server is not accessible from the Umbrella cloud, the query never reaches the destined internal DNS server.