

# Auflösung ungeschützter oder unverschlüsselter Roaming-Client-Modi

## Inhalt

---

[Einleitung](#)

[Ungeschützte und unverschlüsselte Status](#)

[Kommunikationsanforderungen](#)

[Testen der Netzwerkverbindung](#)

[Nur unverschlüsselter Status](#)

---

## Einleitung

In diesem Dokument werden die Bedeutung der Zustände Unprotected und Unencrypted im Umbrella Roaming Client und deren Fehlerbehebung beschrieben.

## Ungeschützte und unverschlüsselte Status

Wenn sich der Umbrella Roaming Client im ungeschützten oder unverschlüsselten Modus befindet, wird das Taskleistensymbol (Windows) oder die Menüleiste (OS X) gelb dargestellt. Der Status wird sowohl als ungeschützt als auch als unverschlüsselt angezeigt.

## Kommunikationsanforderungen

Um Sicherheit und Content-Filterung zu gewährleisten, muss der Umbrella Roaming Client mit Umbrella sowohl über UDP als auch über TCP auf den bereitgestellten Ports und Zielen kommunizieren, zusätzlich zu den HTTP-Zielen, die im Artikel [Roaming Client-Voraussetzungen](#) aufgeführt sind:

Anschluss	Protokolle	IPv4	IPv6
53	UDP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
53	TCP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
443	UDP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35
443	TCP	208.67.222.222, 208.67.220.220	2620:119:53::53, 2620:119:35::35

Der Umbrella Roaming Client kann den Computer nicht schützen, wenn beide Bedingungen gegeben sind:

- Der Computer befindet sich hinter einer Verbindung, die keine DNS-Anfragen von Drittanbietern zulässt.

- Der Computer befindet sich hinter einer Verbindung, für die die standardmäßige Richtlinie für ausgehende Firewall verweigert gilt.

Wenn diese Bedingungen erfüllt sind, stellt der Umbrella Roaming Client die DHCP-delegierten DNS-Server in den Eigenschaften der Netzwerkverbindung wieder her und setzt die Tests fort, bis er Umbrella DNS-Server kontaktieren und die Sicherheits- und Inhaltsfilterung fortsetzen kann. In Zeiträumen, in denen keine Kommunikation mit Umbrella DNS-Servern möglich ist, stehen Richtliniendurchsetzung und Berichterstellung nicht zur Verfügung.

## Testen der Netzwerkverbindung

Um zu überprüfen, ob das Netzwerk die Kommunikation mit Umbrella DNS-Servern zulässt, führen Sie manuell eine DNS-Abfrage durch. Wenn das Netzwerk Abfragen blockiert, lautet die Ausgabe:

```
$ nslookup.opendns.com 208.67.222.222
;; connection timed out; no servers could be reached
```

Wenn der Test erfolgreich war, der Umbrella Roaming Client jedoch weiterhin "Unprotected/Unencrypted" meldet, öffnen Sie ein Support-Ticket und stellen die Ergebnisse eines Diagnosetests bereit. Eine erfolgreiche Abfrage wird angezeigt als:

```
$ nslookup.opendns.com 208.67.222.222
Server: 208.67.222.222
Address: 208.67.222.222#53
```

```
Non-authoritative answer:
Name: .opendns.com
```

## Nur unverschlüsselter Status

Wenn der Umbrella Roaming Client Unverschlüsselt anzeigt, kann er nicht über Port 443/UDP kommunizieren. Aus Sicherheitsgründen wird empfohlen, diesen Port durch die Firewall zu gestatten. Der Client funktioniert jedoch weiterhin ohne verschlüsselte DNS-Abfragen. Weitere Informationen finden Sie im Artikel zu den Voraussetzungen für [Roaming-Clients](#).

## 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.