

Risoluzione delle modalità client mobili non protette o non crittografate

Sommario

[Introduzione](#)

[Stati non protetti e non crittografati](#)

[Requisiti di comunicazione](#)

[Verifica della connettività di rete](#)

[Solo stato non crittografato](#)

Introduzione

Questo documento descrive il significato degli stati Non protetto e Non crittografato in Umbrella Roaming Client e come risolverli.

Stati non protetti e non crittografati

Quando Umbrella Roaming Client è in modalità non protetta o non crittografata, l'icona sull'area di notifica (Windows) o la barra dei menu (OS X) visualizza uno stato giallo. Lo stato viene visualizzato come Non protetto e Non crittografato.

Requisiti di comunicazione

Per garantire la sicurezza e il filtro dei contenuti, il client di roaming Umbrella deve comunicare con Umbrella utilizzando sia UDP che TCP sulle porte e le destinazioni fornite, oltre alle destinazioni HTTP elencate nell'articolo [Prerequisiti client di roaming](#):

Port	Protocollo	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

Il client Umbrella Roaming non è in grado di proteggere il computer se sono presenti entrambe le seguenti condizioni:

- Il computer è dietro una connessione che non consente richieste DNS di terze parti.
- Il computer è dietro una connessione che dispone di un criterio del firewall di negazione in uscita predefinito.

Quando queste condizioni sono soddisfatte, il client Umbrella Roaming ripristina i server DNS delegati tramite DHCP nelle proprietà della connessione di rete e continua i test finché non è in grado di contattare i server DNS Umbrella e riprendere a fornire protezione e filtraggio dei contenuti. Nei periodi in cui la comunicazione con i server DNS Umbrella non è possibile, non sono disponibili funzionalità di applicazione e creazione di rapporti.

Verifica della connettività di rete

Per verificare se la rete consente la comunicazione con i server DNS Umbrella, eseguire manualmente una query DNS. Se la rete blocca le query, l'output è il seguente:

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

Se il test ha esito positivo ma il client Umbrella Roaming riporta comunque "Non protetto/Non crittografato", aprire un ticket di supporto e fornire i risultati di un test diagnostico. Una query riuscita viene visualizzata nel modo seguente:

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

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

Solo stato non crittografato

Se il client Umbrella Roaming visualizza Unencrypted, non può comunicare sulla porta 443/UDP. Per motivi di sicurezza è consigliabile consentire l'utilizzo di questa porta attraverso il firewall, ma il client continua a funzionare senza query DNS crittografate. Per ulteriori informazioni, fare riferimento all'articolo [Prerequisiti per i client mobili](#).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).