# Il modulo Umbrella rimane disabilitato in Secure Client

## Sommario

## Problema

Il modulo Umbrella DNS Security all'interno di Cisco Secure Client (agente VPN AnyConnect) rimane nello stato "Disabilitato" dopo l'applicazione del file del profilo Umbrella a causa di una mancata corrispondenza delle impronte digitali di registrazione del dispositivo. Il problema persiste in vari ambienti di rete, incluse le connessioni degli hotspot personali e degli uffici aziendali.

Gli artefatti diagnostici, come gli screenshot, le acquisizioni di pacchetti DART e i file di acquisizione dei pacchetti, hanno indicato errori di registrazione del dispositivo collegati a una mancata corrispondenza delle impronte digitali nel file OrgInfo.json:

- Nel modulo Umbrella viene visualizzato lo stato "Disabilitato".
- Il problema si verifica dopo l'applicazione del file di profilo Umbrella.
- Il problema si verifica su più reti.
- I registri diagnostici e le acquisizioni dei pacchetti mostrano gli errori di registrazione del dispositivo.

## Ambiente

- Prodotto: Cisco Secure Client (agente VPN AnyConnect) con modulo Umbrella
- Piattaforma: Sistema operativo Windows
- Funzionalità di sicurezza DNS Umbrella
- File di profilo Umbrella e OrgInfo.json interessati
- Ambienti di rete: ufficio aziendale, hotspot personale
- Elementi diagnostici: Pacchetto DART, acquisizione pacchetti, screenshot
- Versione del software: Tutto

## Risoluzione

Questo flusso di lavoro dettagliato risolve lo stato "Disabilitato" del modulo Umbrella correggendo la mancata corrispondenza delle impronte digitali nel file OrgInfo.json e registrando nuovamente il dispositivo con il servizio cloud Umbrella.

### Scaricare un nuovo file OrgInfo.json dal dashboard SSE

Per assicurarsi che la registrazione del dispositivo utilizzi l'impronta digitale corretta:

1. Ottenere un nuovo file OrgInfo.json.
2. Scaricare il file OrgInfo.json aggiornato direttamente dal dashboard Cisco Secure Service Edge (SSE).

## Arrestare Cisco Secure Client - Servizio AnyConnect VPN Agent

Per arrestare il servizio è necessario modificare in modo sicuro i file associati al modulo Umbrella:

Aprire Servizi Windows e arrestare il servizio Cisco Secure Client - AnyConnect VPN Agent.

## Elimina tutto il contenuto dalla cartella del modulo Umbrella

1. Cancellare da questa posizione tutti i dati potenzialmente danneggiati o obsoleti.
2. Elimina tutti i file e le cartelle in:

```
C:/ProgramData/Cisco/Cisco Secure Client/Umbrella/
```

Attenzione: possibile. I dettagli menzionati qui sembrano contenere procedure o comandi che potrebbero causare un impatto significativo se eseguiti. Assicurarsi che le procedure o i comandi sopra menzionati siano stati valutati da uno SME o da una Business Unit prima di eseguire o consigliare.

## Caricare il file New OrgInfo.json

1. Posizionare il file OrgInfo.json appena scaricato nella cartella Umbrella designata.
2. Copiare il nuovo file OrgInfo.json in:

```
C:/ProgramData/Cisco/Cisco Secure Client/Umbrella/
```

## Riavviare il servizio Cisco Secure Client

Reinizializzare Cisco Secure Client per rendere effettive le modifiche. Avviare il servizio Cisco Secure Client - AnyConnect VPN Agent dai servizi Windows.

## (Se il problema persiste) Raccogliere i dati diagnostici per un'ulteriore analisi

Se il dispositivo non riesce ancora a eseguire la registrazione, raccogliere un nuovo bundle DART per facilitare una risoluzione dei problemi più approfondita. Utilizzare lo strumento DART in Cisco Secure Client per raccogliere un nuovo bundle di diagnostica.

Dopo aver eseguito questi passaggi, il modulo Umbrella deve passare da uno stato "Disabilitato" a uno stato operativo, abilitando le funzionalità di sicurezza DNS come previsto.

## Causa

La causa principale del problema è un file OrgInfo.json non valido o obsoleto contenente un valore di impronta digitale del dispositivo non corretto. Questa mancata corrispondenza ha causato richieste di registrazione del dispositivo non riuscite all'API Umbrella, con conseguente disabilitazione del modulo. L'errore è stato confermato dalle voci di registro che mostrano "impronta digitale non corrispondente" e "impossibile creare l'ID dispositivo" durante i tentativi di registrazione.

Esempio di log estratto dai log DART:

```
{"error":"invalid_request","message":"fingerprint does not match","code":400,"code_text":"Bad Request"}
Device Registration: failed to create device id
```

## Contenuto correlato

- Supporto tecnico Cisco e download

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).