

Risolvere i problemi relativi agli errori dei certificati radice Umbrella quando si utilizza Chrome in Windows

Sommario

[Introduzione](#)

[Panoramica](#)

[Disattivazione dei controlli dei certificati Chrome \(solo Windows\)](#)

Introduzione

Questo documento descrive come risolvere i problemi relativi agli errori dei certificati radice Umbrella per *.cisco.com quando si utilizza Chrome su Windows.

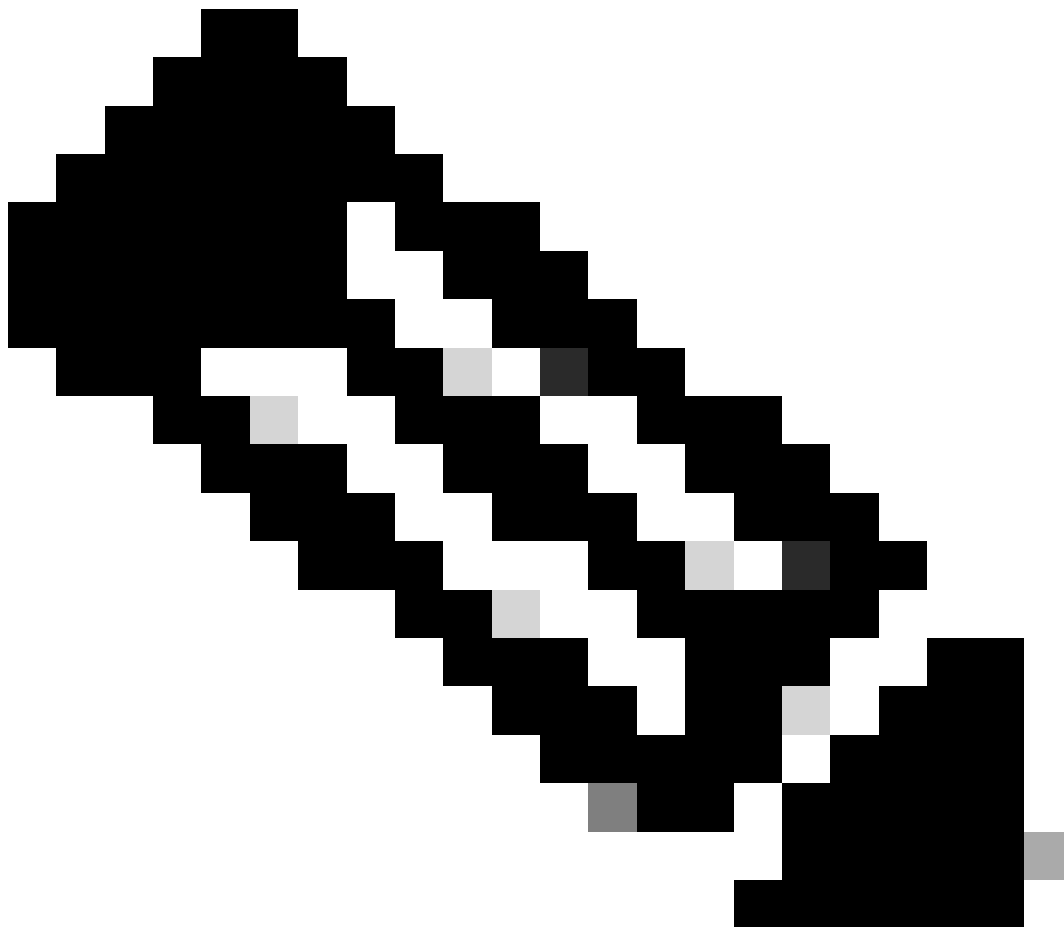
Panoramica

Ora disponiamo di una soluzione più gestibile e duratura per questo problema che si applica a tutti i siti. Anche se le informazioni fornite qui rimangono pertinenti, si consiglia di esplorare la correzione permanente installando la CA radice Cisco, come descritto in questo articolo:

<https://docs.umbrella.com/deployment-umbrella/docs/rebrand-cisco-certificate-import-information>

Questa pagina è una guida per quando un errore certificato per *.cisco.com viene visualizzato in Chrome (per Windows), ma non può essere ignorato aggiungendo un'eccezione certificato.

La causa di questo messaggio è l'implementazione di HTTP Strict Transport Security (HSTS) o il pre-caricato Certificate Pinning nei browser moderni che ne migliora la sicurezza complessiva. Questa sicurezza aggiuntiva per le pagine HTTPS impedisce il funzionamento del meccanismo di blocco delle pagine Umbrella e del blocco bypass quando HSTS è attivo per un sito Web. Per ulteriori informazioni su HSTS, fare riferimento a [questo articolo](#).



Nota: A causa delle modifiche apportate a HSTS, il sistema BPB (Block Page Bypass) non funziona con alcuni siti a causa di errori di certificato non ignorabili. Per consentire a questi siti di funzionare con BPB in Chrome (per Windows), è necessario utilizzare un'opzione speciale quando si avvia il browser. Alcuni siti comuni che non funzionano con BPBin Chrome includono: Facebook, Google Siti come Gmail e YouTube, Dropbox e Twitter. Per un elenco completo dei siti, leggere [qui](#).

Se non si disattivano le verifiche dei certificati Chrome, i tentativi di utilizzare l'opzione Blocca bypass pagina con uno qualsiasi dei siti in questo elenco protetto hanno esito negativo, come mostrato di seguito.

Disattivazione dei controlli dei certificati Chrome (solo Windows)

Per forzare Chrome a ignorare questi errori, è necessario impostare il collegamento per Chrome per avviare l'applicazione con questo switch:

--ignore-certificate-errors

Si noti che Google può scegliere di rimuovere questa funzione in qualsiasi momento e quindi è consigliato solo finché è disponibile:

Per aggiungere questo flag della riga di comando a Chrome, fare clic con il pulsante destro del mouse sul collegamento dell'icona Chrome, selezionare "Proprietà" e aggiungerlo a e selezionare "Proprietà", quindi aggiungerlo alla destinazione come mostrato di seguito:

Una volta aggiunto questo flag, è possibile utilizzare BPB normalmente sui siti nell'elenco HSTS precaricato per poterli ignorare.

In questo esempio, sebbene twitter.com sia nell'elenco HSTS precaricato, ignorando l'avviso del certificato è possibile utilizzare Blocca bypass pagina come progettato.

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).