# Dépannage des erreurs de certificat HSTS et d'épinglage

## Table des matières



## Introduction

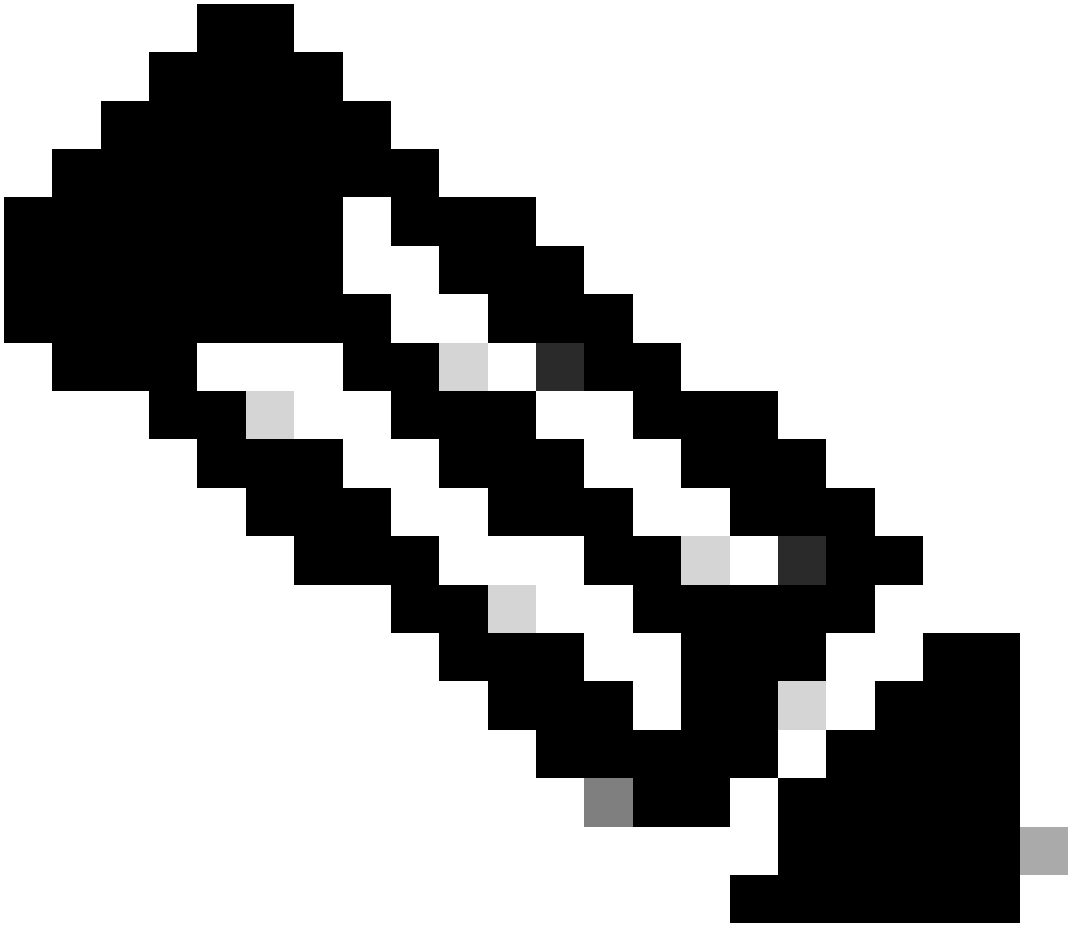
Ce document décrit comment effacer une erreur de certificat « Votre connexion n'est pas approuvée/n'est pas privée » qui ne peut pas être contournée.

## Erreur de certificat

Lorsqu'une erreur de certificat pour `*.opendns.com` ou `*.cisco.com` apparaît mais ne peut pas être contournée en ajoutant une exception de certificat comme indiqué dans la documentation Cisco Umbrella Gérer le certificat racine Cisco Umbrella, utilisez ces étapes pour permettre à l'erreur de certificat d'être effacée.

Lorsque vous ne pouvez pas contourner l'erreur de certificat en ajoutant une exception, cela est dû à l'implémentation de HTTP Strict Transport Security (HSTS) ou à l'épinglage de certificat préchargé dans les navigateurs modernes. La communication entre certains navigateurs et certains sites Web s'effectue de manière à inclure l'obligation d'utiliser HTTPS et aucune exception ou contournement n'est possible. Cette sécurité supplémentaire pour les pages HTTPS empêche le fonctionnement de la page de blocage Umbrella et du mécanisme de page de blocage de contournement lorsque HSTS est actif pour un site Web.

Par conséquent, la page en question n'est pas accessible via Block Page Bypass (BPB) (en fait, l'écran Bypass peut même ne pas apparaître). Ces méthodes peuvent autoriser l'accès à la connexion BPB, mais après la connexion, l'erreur de certificat réapparaît et refuse l'accès. Revoyez le reste de cet article si vous voyez une erreur de certificat dans Google Chrome, Mozilla Firefox, Safari qui ne peut pas être contourné et vous essayez d'accéder à la connexion de contournement.



Remarque : Une solution à ce problème, plus facile à gérer et persistante pour tous les sites, est désormais disponible.

Par conséquent, ces informations sont toujours applicables, mais peuvent désormais être contournées avec une solution permanente. Essayez d'installer l'autorité de certification racine Cisco via la documentation Cisco Umbrella : Gérer le certificat racine Cisco Umbrella

---

IMPORTANT : Si le domaine est sur la liste épinglée HSTS, une exception ne peut pas être ajoutée car la liste est effectivement non contournable si vous exécutez Chrome, Safari ou Firefox (Internet Explorer (IE) n'est pas affecté). Bloquer le contournement de page ne fonctionne pas pour des sites comme celui-ci. Pour une liste complète des services utilisant HSTS par ces trois navigateurs, s'il vous plaît lire le Google Chromium Code Search. Les services notables de cette liste sont les suivants :

- Google (et les ressources Google, telles que Gmail, Youtube ou Google Docs)
- Dropbox

- Twitter
- Facebook

Si vous ou vos utilisateurs rencontrez un problème et que vous souhaitez que des modifications soient apportées à l'option Bloquer le contournement de la page afin de résoudre ce problème, envoyez un e-mail à umbrella-support@cisco.com ou à votre responsable de compte pour soumettre une demande de fonctionnalité. Nos équipes d'ingénierie et de gestion des produits sont conscientes des difficultés liées aux certificats et au contournement des pages de blocage et testent d'autres reconceptions de cette fonctionnalité.

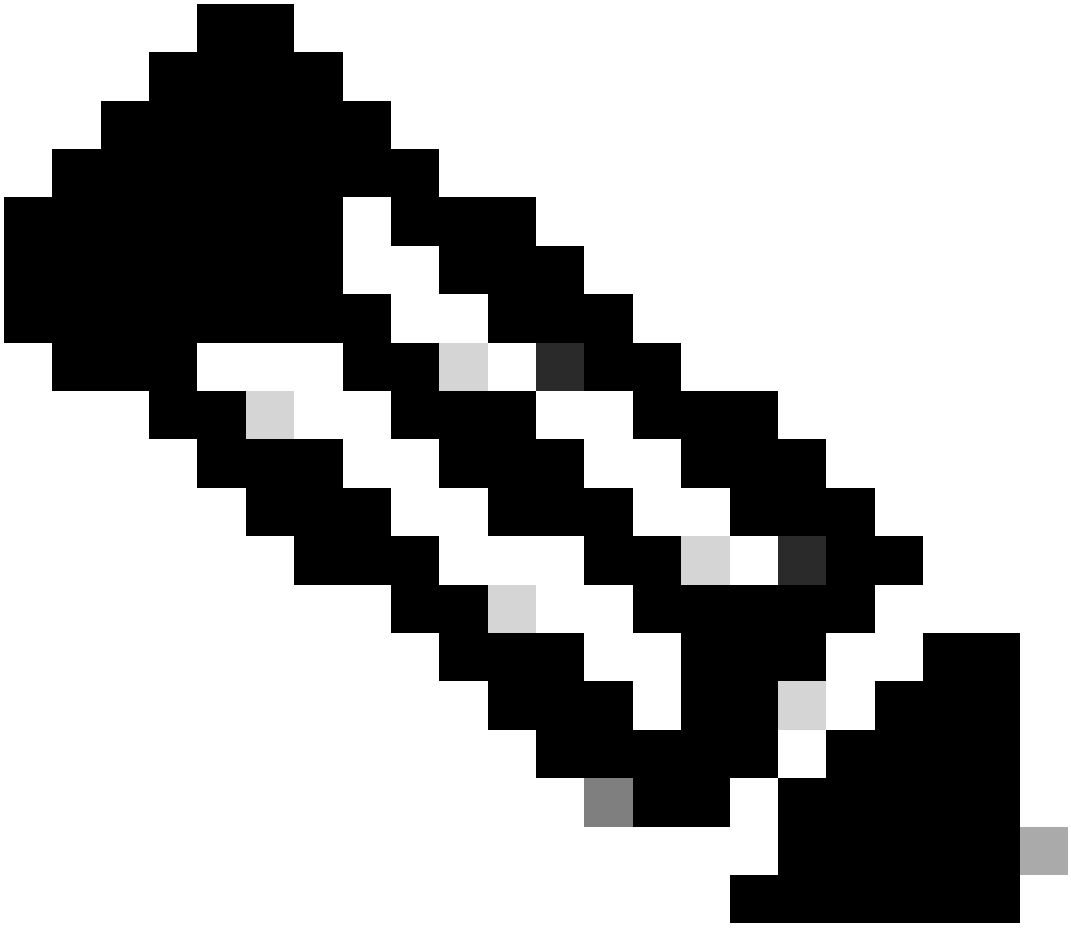
# Solutions possibles

Il y a quelques façons de résoudre ces problèmes. Tout d'abord, ces sections montrent comment utiliser des politiques plus granulaires pour contourner ce problème.  Deuxièmement, vous pouvez utiliser des configurations de navigateur, mais celles-ci sont isolées d'un sous-ensemble des navigateurs affectés par ce problème.

## Gestion des stratégies et client d'itinérance

Il peut y avoir des problèmes avec votre configuration réseau ou votre politique d'utilisation acceptable (HR) qui empêchent cette solution. La gestion des politiques n'est pas une solution efficace si les utilisateurs ne sont autorisés à visiter ces domaines qu'à des heures données (par exemple pendant leur pause déjeuner). Umbrella ne peut pas fournir une application de politique basée sur le temps avec notre service, de sorte que simplement permettre à un utilisateur d'accéder au site tout le temps pourrait être problématique. Sur un ordinateur partagé, tel qu'un terminal public, le client d'itinérance Umbrella ne peut pas différencier les utilisateurs et ne peut pas facilement autoriser les bons domaines pour les bonnes personnes.

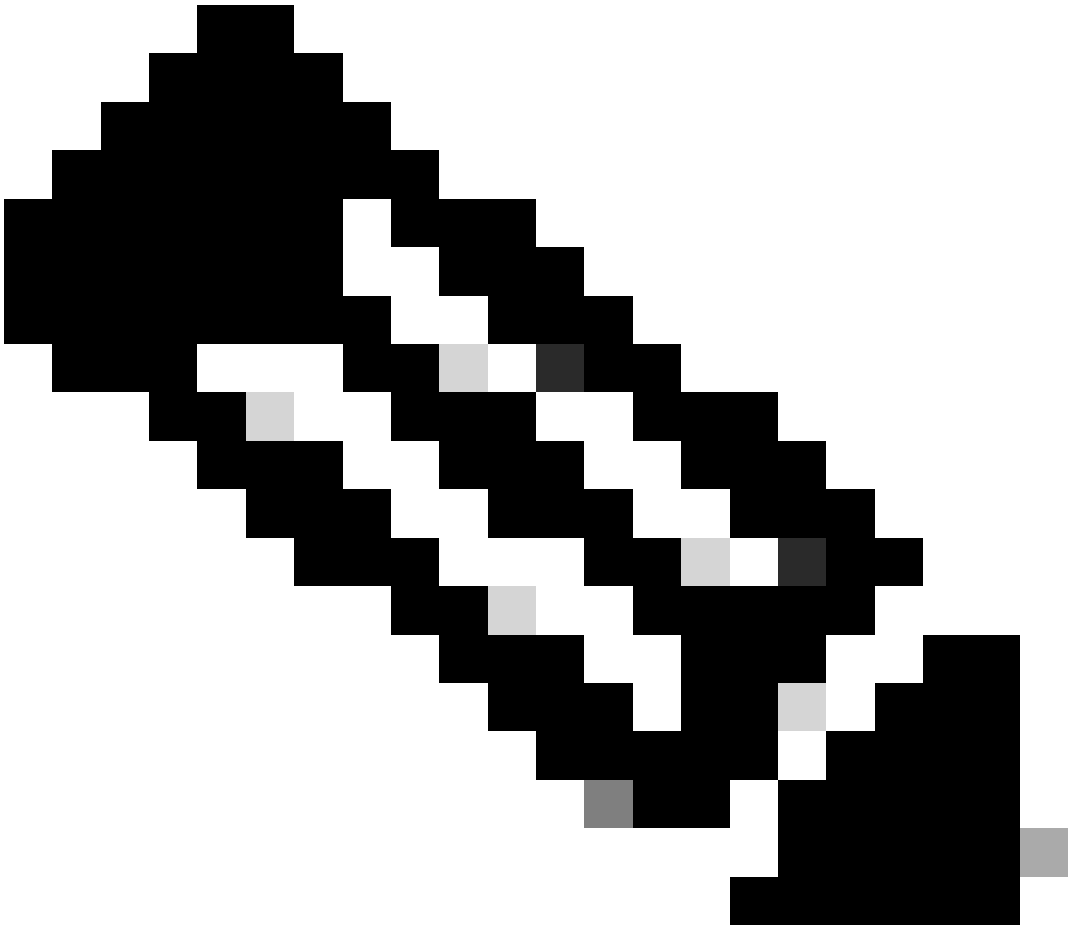
La gestion des stratégies n'est pas aussi efficace lorsque l'on considère des identités non granulaires, telles que Sites ou Réseaux, à moins que l'administrateur ne soit à l'aise pour accorder le même accès à tous les utilisateurs de ce réseau. La gestion des stratégies fonctionne de manière optimale lorsqu'elle est appliquée à un sous-ensemble d'utilisateurs autorisés à accéder à des sites alors que le reste du réseau ne peut pas y accéder, et lorsqu'il s'agit de distinguer ces utilisateurs en installant le client itinérant sur leurs ordinateurs et en appliquant la hiérarchie de stratégies appropriée.



Remarque : Cisco a annoncé la fin de vie d'Umbrella Roaming Client le 2 avril 2024. La date limite d'assistance pour Umbrella Roaming Client est le 2 avril 2025. Toutes les fonctionnalités d'Umbrella Roaming Client sont actuellement disponibles dans Cisco Secure Client. Cisco propose des innovations à venir dans le domaine de la sécurité client Cisco uniquement. Nous recommandons aux clients de commencer dès maintenant à planifier leur migration. Reportez-vous à cet article de la Base de connaissances pour obtenir des conseils sur la façon de migrer du client d'itinérance Umbrella vers le client sécurisé Cisco.

Une bonne gestion des politiques est la meilleure solution à ce problème, car le navigateur ne reçoit pas de réponse de validation en échec. Si certains de vos utilisateurs sont autorisés à accéder à des sites qu'ils devraient normalement utiliser pour l'accès à Bloquer le contournement de page, vous pouvez configurer une stratégie distincte pour ces utilisateurs et ajouter les domaines qu'ils peuvent utiliser à la liste verte. Comme les requêtes des utilisateurs ne sont jamais bloquées, le navigateur ne reçoit jamais de requête d'un domaine avec un certificat incompatible. Vous pouvez utiliser le client Umbrella Roaming pour appliquer ces politiques spécifiques. Cela signifie que vous

placez certains domaines dans une liste d'autorisation pour certains utilisateurs à tout moment de la journée afin de contourner ces erreurs.



Remarque : Le client d'itinérance Umbrella est un moyen efficace de distribuer des stratégies particulières à plusieurs utilisateurs, mais si vous avez activé l'intégration Active Directory(AD), vous pouvez également appliquer ces stratégies autorisées à des utilisateurs AD particuliers.

## Ignorer les erreurs d'exception de certificat (Chrome pour Windows uniquement)

Seul Chrome pour Windows peut être configuré pour ignorer les erreurs d'exception de certificat, ce qui atténue cette erreur. Le navigateur est invité à ignorer l'erreur et la page de blocage Umbrella normale s'affiche à la place.

IMPORTANT : Cette méthode est plus risquée que l'ajustement de votre gestion des stratégies,

car le navigateur est configuré pour ignorer les erreurs de certificat. Il est possible que, par conséquent, le navigateur puisse être soumis à des attaques de type « man-in-the-middle » (MiTM). Par conséquent, nous ne pouvons pas recommander cette approche comme une approche sécurisée pour traiter cette erreur, mais il s'agit d'une solution de contournement.

Ces modifications de configuration doivent être effectuées sur chaque ordinateur, ce qui complique la tâche pour les environnements à grande échelle, mais cela fonctionne.

## Firefox, Safari et Chrome pour Mac OS X

Firefox, Safari et Chrome pour Mac OS X ne peuvent pas être configurés pour ignorer les erreurs d'exceptions de certificats pour les domaines épinglés, et respectent toujours la liste HSTS. Il n'y a aucune solution connue pour ces erreurs.

## Internet Explorer

Internet Explorer (IE) n'implémente pas les restrictions HSTS. Par conséquent, IE n'a pas besoin d'être configuré et n'affiche pas cette erreur. Cela peut être modifié dans les versions futures d'IE si Microsoft choisit d'implémenter HSTS dans le navigateur.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.