Fehlerbehebung bei HSTS- und Pinning-Zertifikatfehlern

Inhalt

Einleitung

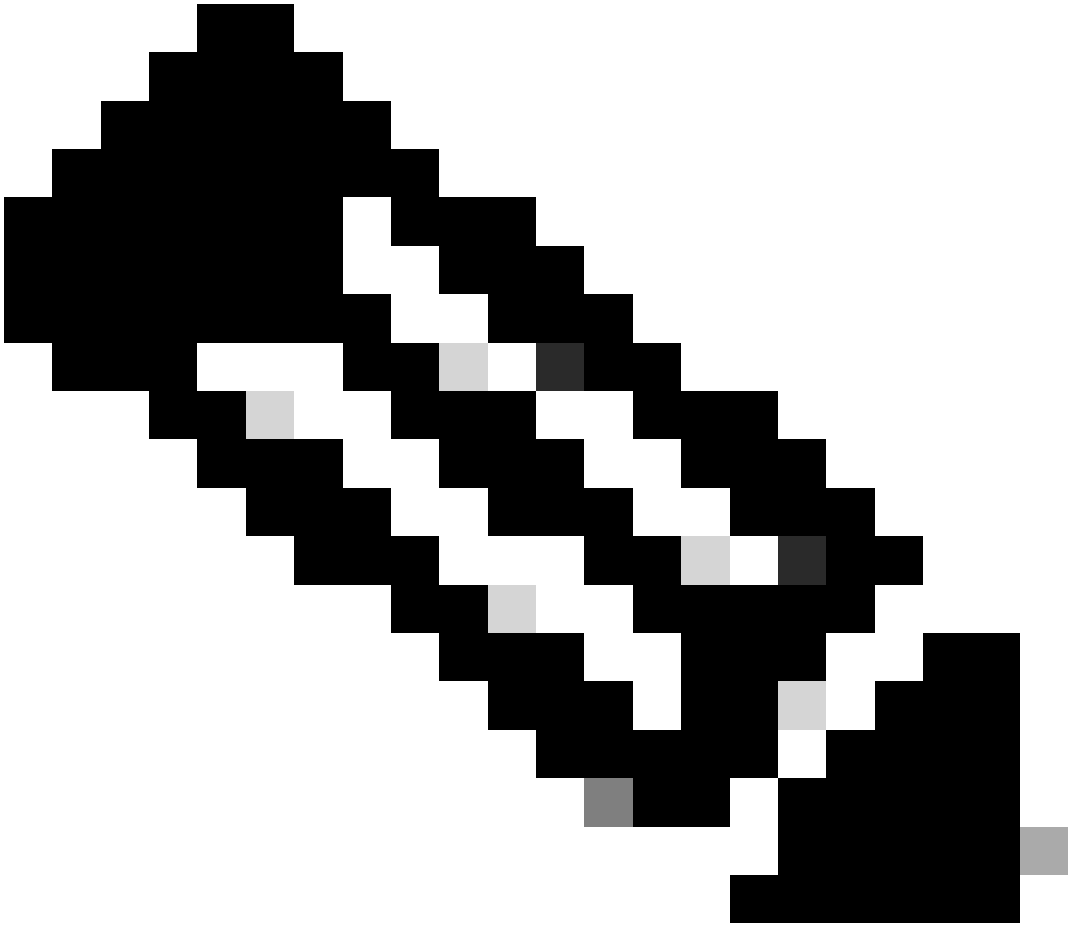
In diesem Dokument wird beschrieben, wie Sie den Zertifikatfehler "Ihre Verbindung ist nicht vertrauenswürdig/nicht privat" löschen, der nicht umgangen werden kann.

Zertifikatfehler

Wenn ein Zertifikatfehler für `*.opendns.com` oder `*.cisco.com` angezeigt wird, jedoch nicht umgangen werden kann, indem eine Zertifikatausnahme gemäß der Dokumentation Verwalten des Cisco Umbrella Root-Zertifikats hinzugefügt wird, führen Sie die folgenden Schritte aus, damit der Zertifikatfehler gelöscht werden kann.

Wenn Sie den Zertifikatfehler nicht umgehen können, indem Sie eine Ausnahme hinzufügen, liegt dies an der Implementierung von HTTP Strict Transport Security (HSTS) oder der vorinstallierten Zertifikatpinning in modernen Browsern. Die Kommunikation zwischen bestimmten Browsern und bestimmten Websites erfolgt auf eine Weise, die die Anforderung zur Verwendung von HTTPS beinhaltet und keine Umgehung oder Ausnahme möglich ist. Diese zusätzliche Sicherheit für HTTPS-Seiten verhindert, dass die Umbrella-Blockseite und der Umgehungs-Blockseitenmechanismus funktionieren, wenn HSTS für eine Website aktiv ist.

Daher kann auf die betreffende Seite nicht über Block Page Bypass (BPB) zugegriffen werden (der Bypass-Bildschirm wird möglicherweise nicht einmal angezeigt). Diese Methoden erlauben möglicherweise den Zugriff auf die BPB-Anmeldung, aber nach der Anmeldung wird der Zertifikatfehler erneut angezeigt und der Zugriff verweigert. Lesen Sie den Rest dieses Artikels, wenn Sie ein Zertifikat Fehler in Google Chrome, Mozilla Firefox, Safari, die nicht umgangen werden können und Sie versuchen, den Bypass-Login zugreifen sehen.



Anmerkung: Eine Lösung für dieses Problem, die einfacher zu verwalten und dauerhaft für alle Standorte ist jetzt verfügbar.

Diese Informationen sind somit weiterhin gültig, können aber nun mit einer dauerhaften Lösung umgangen werden. Versuchen Sie, die Cisco Root CA über die Cisco Umbrella-Dokumentation zu installieren: Cisco Umbrella Root-Zertifikat verwalten

---

WICHTIG: Wenn sich die Domäne in der Liste der per HSTS fixierten Domänen befindet, kann keine Ausnahme hinzugefügt werden, da die Liste praktisch nicht umgangen werden kann, wenn Sie Chrome, Safari oder Firefox ausführen (Internet Explorer (IE) ist davon nicht betroffen). Blockieren der Seitenumgehung funktioniert nicht für solche Sites. Eine vollständige Liste der Dienste, die HSTS von diesen drei Browsern verwenden, finden Sie in der Google Chromium Code Search. Zu den wichtigsten Services in dieser Liste gehören:

- Google (und Google-Ressourcen wie Gmail, Youtube oder Google Docs)
- Dropbox
- Twitter

- Facebook

Wenn dies ein Problem für Sie oder Ihre Benutzer verursacht und Sie Änderungen am Block Page Bypass (Seitenumgehung blockieren) sehen möchten, um dieses Problem zu beheben, senden Sie eine E-Mail an umbrella-support@cisco.com oder Ihren Account Manager, um eine Funktionsanforderung zu senden. Unsere Produktmanagement- und Technikerteams sind sich der Schwierigkeiten mit Zertifikaten und der Blockseiten-Umgehung bewusst und testen alternative Neugestaltungen dieser Funktion.

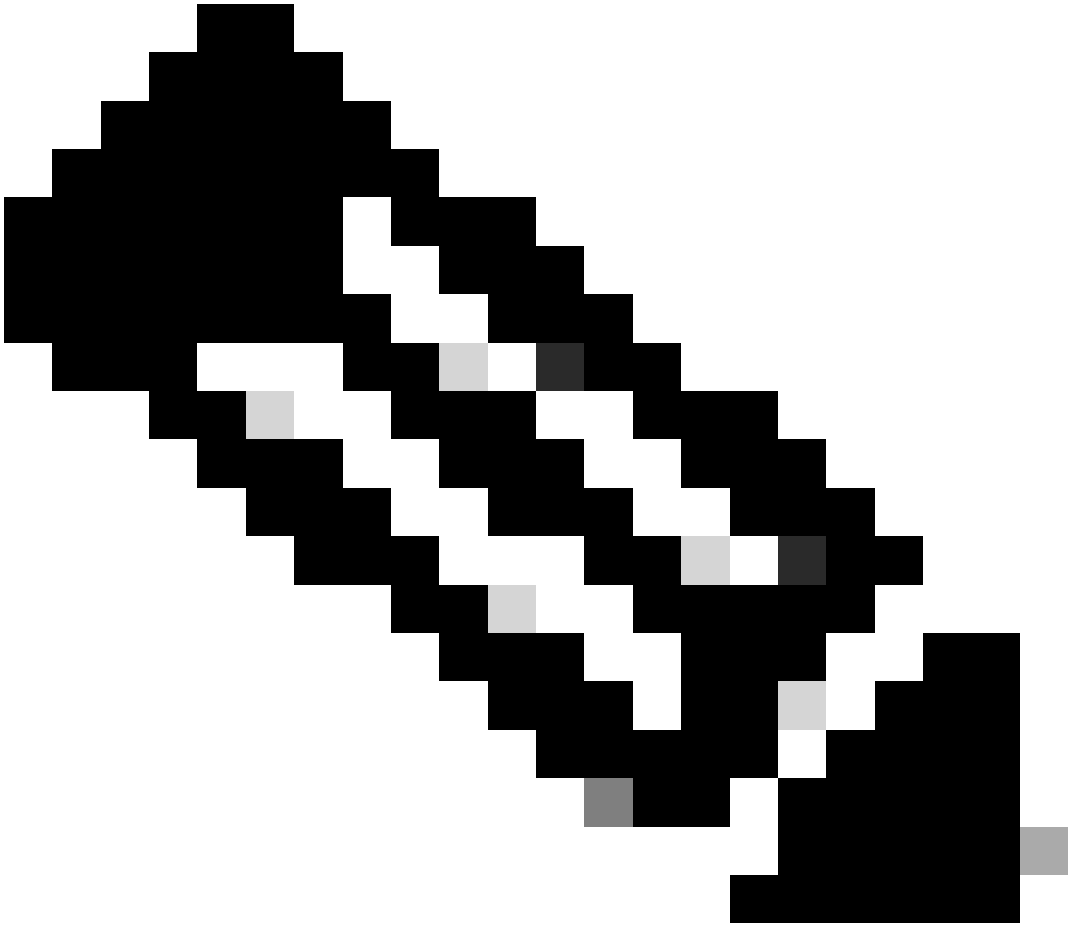
Mögliche Lösungen

Es gibt einige Möglichkeiten, diese Probleme zu lösen. Zunächst zeigen diese Abschnitte, wie Sie dieses Problem mit präziseren Richtlinien umgehen können. Zweitens können Sie Browserkonfigurationen verwenden, die jedoch auf einen Teil der von diesem Problem betroffenen Browser beschränkt sind.

Richtlinienmanagement und Roaming-Client

Möglicherweise liegt ein Problem mit der Netzwerkkonfiguration oder der Richtlinie für die akzeptable Nutzung vor, die diese Lösung verhindert. Das Richtlinienmanagement ist keine effektive Lösung, wenn Benutzer diese Domänen nur zu bestimmten Zeiten (z. B. in der Mittagspause) besuchen dürfen. Umbrella kann keine zeitbasierte Richtlinienanwendung mit unserem Service bereitstellen, sodass es problematisch sein könnte, einem Benutzer den ständigen Zugriff auf die Website zu ermöglichen. Auf einem gemeinsam genutzten Computer, z. B. einem öffentlichen Terminal, kann der Umbrella-Roaming-Client nicht zwischen Benutzern unterscheiden und nicht einfach die richtigen Domänen für die richtigen Personen zulassen.

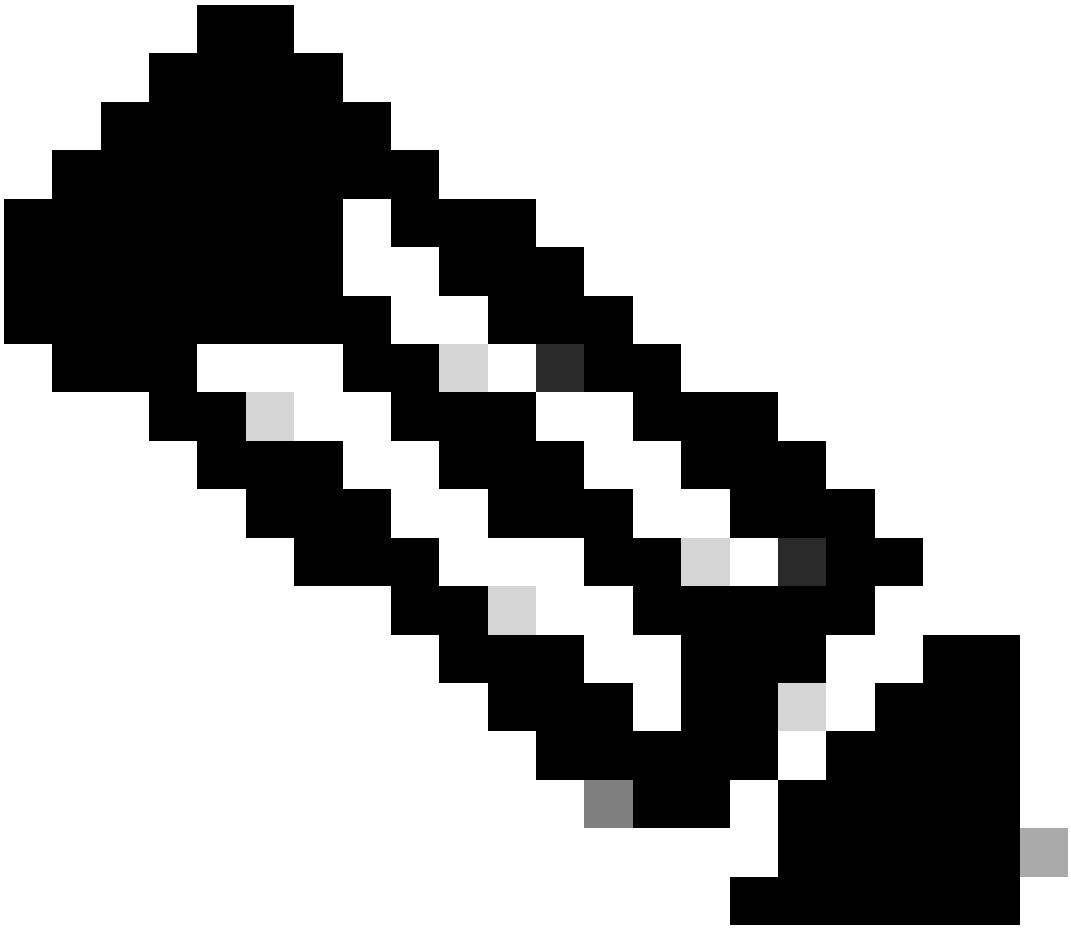
Die Richtlinienverwaltung ist bei nicht detaillierten Identitäten wie Standorten oder Netzwerken nicht so effektiv, es sei denn, der Administrator gibt allen Benutzern dieses Netzwerks den gleichen Zugriff. Die Richtlinienverwaltung funktioniert am besten, wenn sie auf eine Untergruppe von Benutzern angewendet wird, die auf Standorte zugreifen dürfen, während das übrige Netzwerk nicht darauf zugreifen kann, und wenn diese Benutzer herausgegriffen werden, indem der Roaming-Client auf ihren Computern installiert und die entsprechende Richtlinienhierarchie angewendet wird.



Anmerkung: Cisco gab am 2. April 2024 das End-of-Life für Umbrella Roaming Client bekannt. Support für Umbrella Roaming Client ist am 2. April 2025 eingestellt. Alle Umbrella Roaming Client-Funktionen sind derzeit im Cisco Secure Client verfügbar. Cisco bietet zukünftige Innovationen nur für den Cisco Secure Client an. Wir empfehlen unseren Kunden, ihre Migration jetzt zu planen und zu planen. Informationen zur Migration vom Umbrella Roaming Client zum Cisco Secure Client finden Sie in diesem KB-Artikel.

Eine ordnungsgemäße Richtlinienverwaltung ist die beste Lösung für dieses Problem, da der Browser von vornherein keine fehlgeschlagene Validierungsantwort erhält. Wenn einige Ihrer Benutzer auf Websites zugreifen dürfen, die sie normalerweise mithilfe von Seitenumgehung blockieren aufrufen müssten, können Sie stattdessen eine separate Richtlinie für diese Benutzer konfigurieren und die Domänen, die sie verwenden dürfen, der Zulassungsliste hinzufügen. Da die Anfragen der Benutzer niemals blockiert werden, erhält der Browser niemals eine Anfrage von einer Domain mit einem nicht übereinstimmenden Zertifikat. Sie können den Umbrella Roaming Client verwenden, um diese spezifischen Richtlinien bereitzustellen. Das bedeutet, dass Sie bestimmte Domänen für bestimmte Benutzer zu jeder Tageszeit in eine Zulassungsliste aufnehmen,

um diese Fehler zu umgehen.



Anmerkung: Der Umbrella-Roaming-Client stellt eine effektive Möglichkeit dar, bestimmte Richtlinien an mehrere Benutzer zu verteilen. Wenn Sie jedoch die Active Directory(AD)-Integration aktiviert haben, können Sie diese zulässigen Richtlinien auch auf bestimmte AD-Benutzer anwenden.

Zertifikatausnahmefehler werden ignoriert (nur Chrome für Windows)

Nur Chrome für Windows kann so konfiguriert werden, dass Zertifikatausnahmefehler ignoriert werden, wodurch dieser Fehler gemindert wird. Der Browser wird angewiesen, den Fehler zu ignorieren, und stattdessen wird die normale Umbrella-Block-Seite angezeigt.

WICHTIG: Diese Methode ist riskanter als die Anpassung der Richtlinienverwaltung, da der Browser so konfiguriert ist, dass er Zertifikatfehler ignoriert. Es ist möglich, dass der Browser

dadurch einem Man-in-the-Middle-Angriff (MiTM) ausgesetzt ist. Daher können wir diesen Fehler nicht als sicheren Ansatz empfehlen, er ist jedoch umgehbar.

Diese Konfigurationsänderungen müssen für jeden Computer einzeln vorgenommen werden, was große Umgebungen erschwert, aber es funktioniert.

Firefox, Safari und Chrome für Mac OS X

Firefox, Safari und Chrome für Mac OS X können nicht so konfiguriert werden, dass Zertifikatausnahmefehler für angeheftete Domänen ignoriert werden, und berücksichtigen immer die HSTS-Liste. Es gibt keine bekannte Problemumgehung für diese Fehler.

Internet-Explorer

Internet Explorer (IE) implementiert keine HSTS-Einschränkungen. Aus diesem Grund muss IE nicht konfiguriert werden, und dieser Fehler wird nicht angezeigt. Dies kann sich in zukünftigen IE-Versionen ändern, wenn Microsoft HSTS im Browser implementiert.

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.