Troubleshoot HSTS and Pinning Certificate Errors

Contents

Introduction

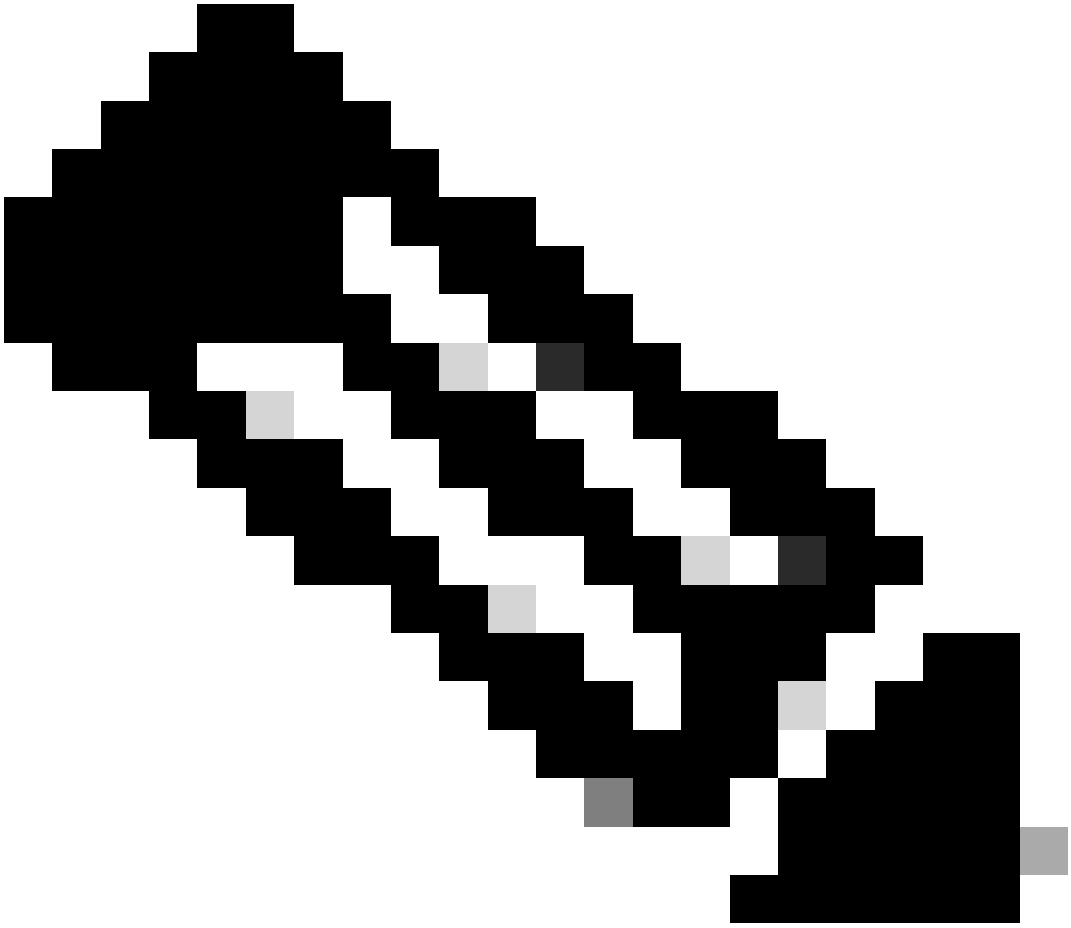
This document describes how to clear a "Your Connection is Untrusted/Not Private" certificate error that cannot be bypassed.

Certificate Error

When a certificate error for `*.opendns.com` or `*.cisco.com` appears but cannot be bypassed by adding a certificate exception as outlined in the Cisco Umbrella documentation Manage the Cisco Umbrella Root Certificate, use these steps to allow the certificate error to be cleared.

When you cannot bypass the certificate error by adding an exception, this is because of the implementation of HTTP Strict Transport Security (HSTS) or pre-loaded Certificate Pinning in modern browsers. Communication between certain browsers and certain websites is done in a way that includes the requirement to use HTTPS and no bypass or exception is possible. This extra security for HTTPS pages prevents the Umbrella block page and bypass block page mechanism from working when HSTS is active for a website.

As a result, the page in question cannot be accessed through Block Page Bypass (BPB) (in fact, the Bypass screen may not even appear). These methods may allow access to the BPB login, but after the login, the certificate error reappears and denies access. Review the rest of this article if you are seeing a certificate error in Google Chrome, Mozilla Firefox, Safari that cannot be bypassed and you are trying to access the bypass login.



Note: A solution for this problem that is easier to manage and persistent for all sites is now available.

As a result, this information is still applicable but can now be worked around with a permanent solution. Try installing the Cisco Root CA via the Cisco Umbrella documentation: Manage the Cisco Umbrella Root Certificate

---

IMPORTANT: If the domain is on the HSTS pinned list, an exception **cannot** be added since the list is effectively non-bypassable if you are running Chrome, Safari, or Firefox (Internet Exporer (IE) is not affected). Block Page Bypass does not work for sites like this. For a complete list of services using HSTS by these three browsers, please review the Google Chromium Code Search. Notable services in this list include:

- Google (and Google resources, such as Gmail, Youtube, or Google Docs)
- Dropbox
- Twitter
- Facebook

If this is causing a problem for you or your users and you would like to see changes to Block Page Bypass to help alleviate this issue, please email umbrella-support@cisco.com or your Account Manager to submit a feature request. Our product management and engineering teams are aware of difficulties with certificates

and block page bypass and are testing alternative redesigns of this feature.

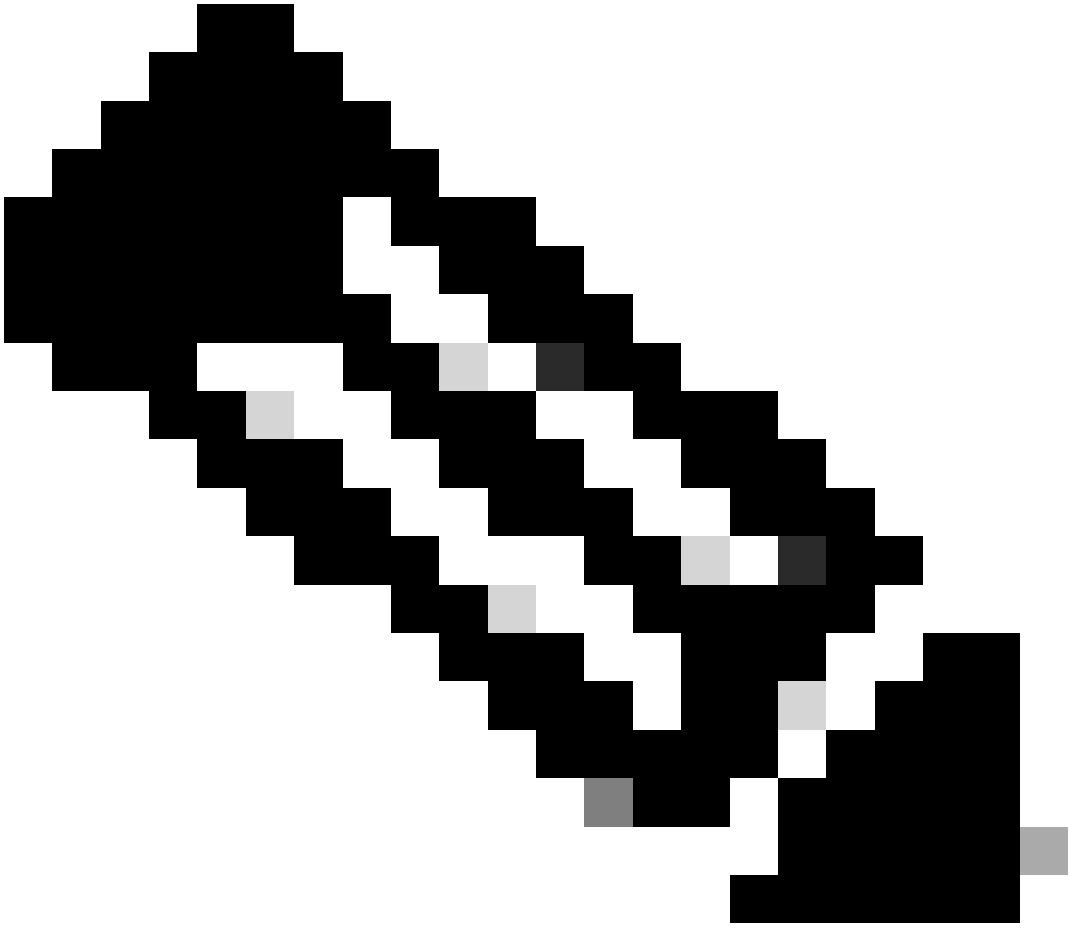
Possible Solutions

There are a few ways to resolve these issues. First, these sections demonstrate how to use more granular policies to work around this issue. Second, you can use browser configurations, but these are isolated to a subset of the browsers affected by this issue.

Policy management and the roaming client

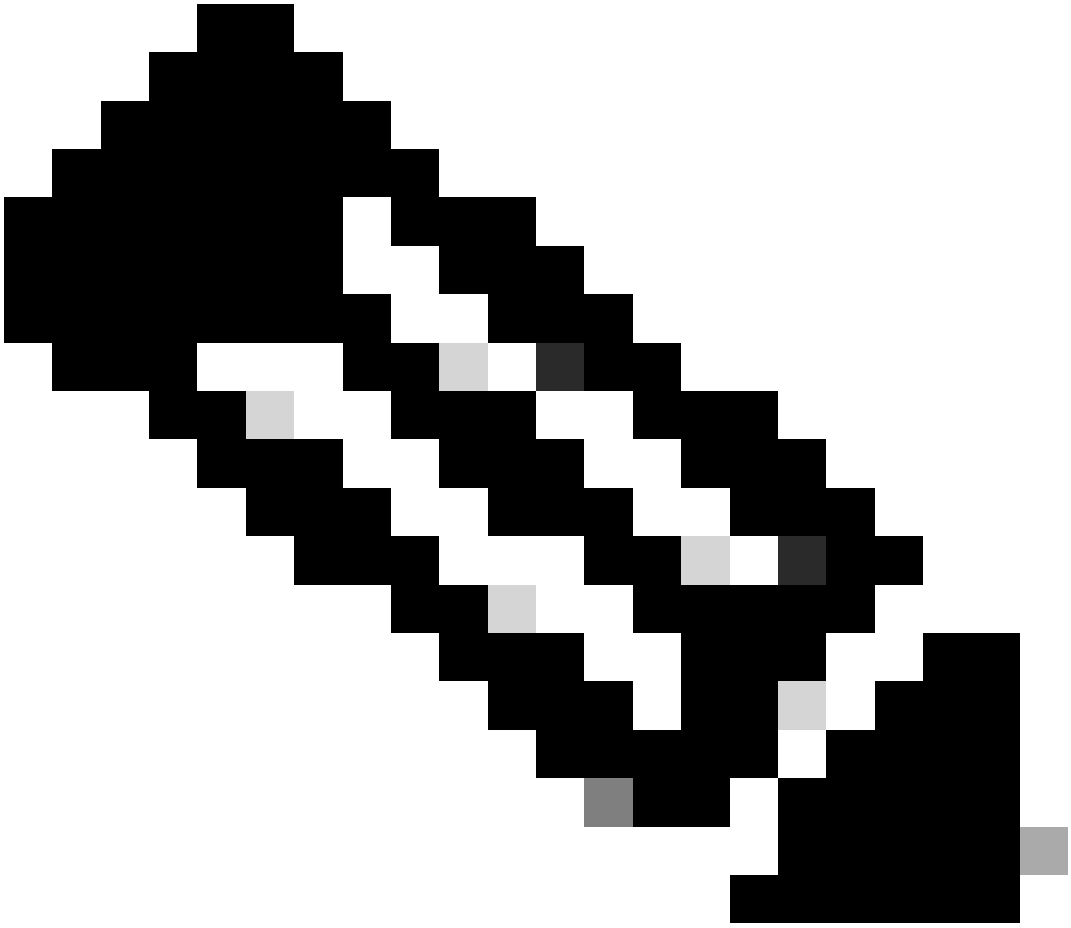
There can be issues with your network configuration or acceptable usage (HR) policy that prevents this solution. Policy management is not an effective solution if users are allowed to visit these domains only at given times (such as during their lunch break). Umbrella cannot provide a time-based policy application with our service, so simply allowing a user to access the site all the time could be problematic. On a shared computer, such as a public terminal, the Umbrella roaming client cannot differentiate between users and cannot easily allow the right domains for the right people.

Policy management is not as effective when considering non-granular identities, such as Sites or Networks, unless the administrator is comfortable giving all users of that network the same access. Policy management works best when applied to a subset of users that are allowed to access sites while the rest of the network cannot, and singling out those users by installing the roaming client on their machines and applying the proper policy hierarchy.



Note: Cisco announced the End-of-Life for Umbrella Roaming Client on April 2, 2024. Last Date of Support for Umbrella Roaming Client is April 2, 2025. All Umbrella Roaming Client functionality is currently available in Cisco Secure Client. Cisco is providing future innovations in Cisco Secure Client only. We recommend that customers begin planning and scheduling their migration now. Please refer to this KB article for guidance on how to migrate from the Umbrella Roaming Client to Cisco Secure Client.

Proper policy management is the best solution to this problem because the browser does not receive a failed validation response in the first place. If some of your users are permitted to access sites that they would normally need to use Block Page Bypass to access, you can instead configure a separate policy for these users and add the domains that they can be allowed to use to the Allow List. Since the users' requests are never blocked, the browser never receives a request from a domain with a mismatched certificate. You can use the Umbrella Roaming Client to deliver these specific policies. This means that you are putting certain domains in an allow list for certain users at all times of the day to work around these errors.



Note: The Umbrella roaming client is an effective way to distribute particular policies to multiple users, but if you have enabled Active Directory(AD) integration, you can apply these permitted policies to particular AD users as well.

Ignoring Certificate Exception errors (Chrome for Windows only)

Only Chrome for Windows can be configured to ignore Certificate Exception errors, which mitigates this error. The browser is told to ignore the error and the normal Umbrella block page is seen instead.

IMPORTANT: This method is riskier than adjusting your policy management because the browser is configured to ignore certificate errors. It is possible that as a result, the browser can be subject to man-in-the-middle (MiTM) attacks. As a result, we cannot recommend this as a secure approach to dealing with this error but it is a workaround.

These configuration changes must be made on a per-computer basis, which makes it difficult for large scale environments, but it does work.

Firefox, Safari and Chrome for Mac OS X

Firefox, Safari and Chrome for Mac OS X **cannot** be configured to ignore certificate exceptions errors for pinned domains, and always honors the HSTS list. There is no known workaround for this these errors.

Internet Explorer

Internet Explorer (IE) does not implement HSTS restrictions. As a result, IE does not need to be configured and does not display this error. This is subject to change in future versions of IE ifMicrosoft chooses to implement HSTS in the browser.