Resolve 516 Upstream Certificate CN Mismatch Error

Contents

Introduction

This document describes how to resolve a 516 Upstream Certificate CN Mismatch error.

Issue

When the Umbrella Secure Web Gateway (SWG) proxy is configured to perform HTTPS Inspection, a user can receive a **516 Upstream Certificate CN Mismatch** error page when browsing to a website using an HTTPS URL.

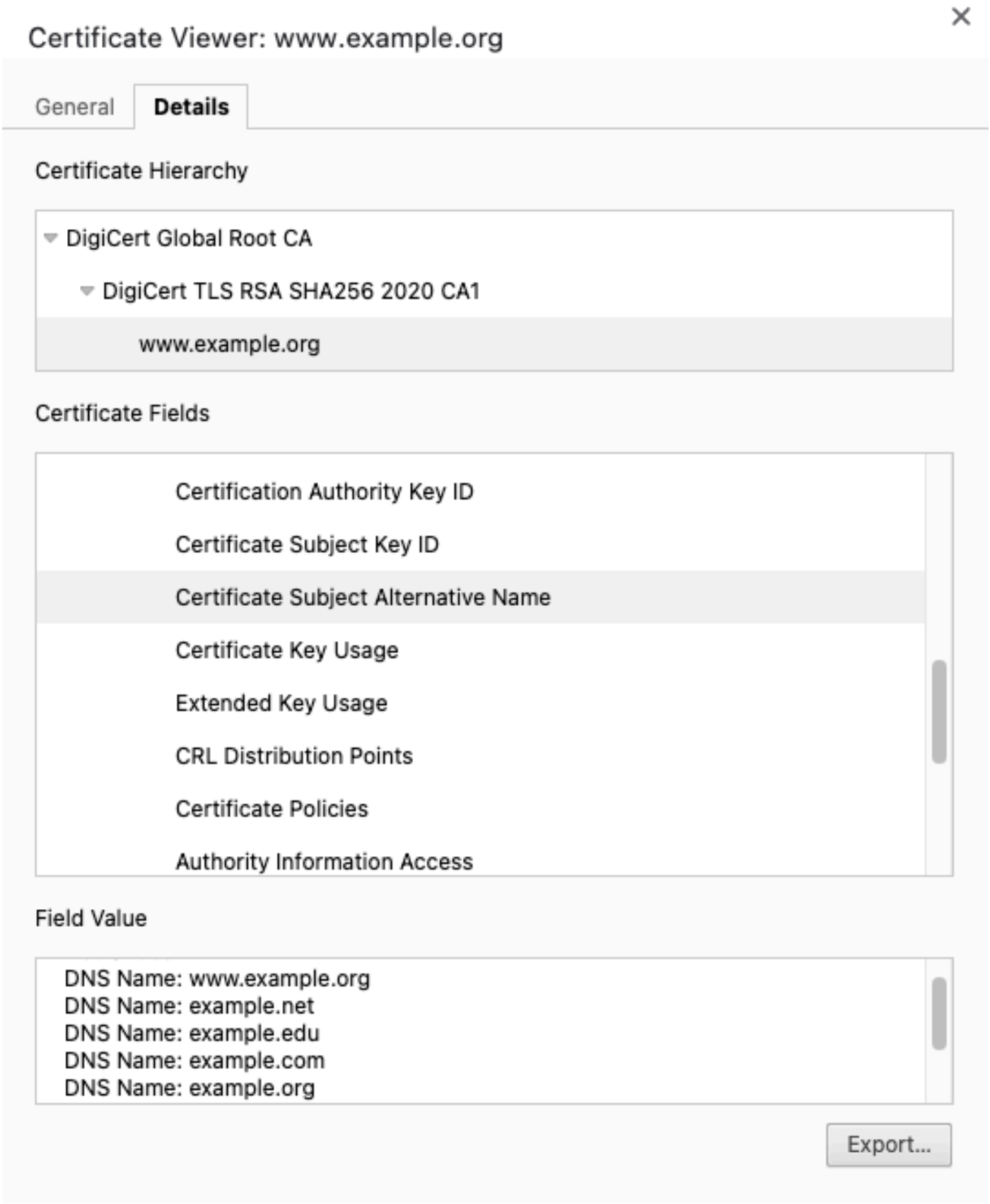
This error does not indicate a problem with the Common Name (CN) attribute in the website certificate's Subject field. Rather, the issue pertains to the DNS Name attribute in the Subject Alternative Names (SAN) extension of a certificate.

After reviewing this article, if you cannot identify the reason for the 516 error page, please contact Umbrella technical support and provide us with the information specified in the **Certificate Identity Errors** section in this document.

Certificate Identity Mechanics

When requesting an HTTPS URL, a browser or other web client sends the domain name in the URL to the web server via the Server Name Indication (SNI) extension in the Client Hello message of the TLS negotiation. The server uses this SNI value to select the server certificate to return to the client, since a server often hosts multiple websites and can have different certificates for some or all of the sites.

When the server certificate is received by the web client, the client verifies that the the certificate is the correct one for the request by comparing the requested domain name to the domain name(s) in the **DNS Name** attributes of the certificate's **Subject Alternative Names** extension. This image shows these SANs in a server certificate.



16796247745556

This web server returns this certificate in response to requests with these SNI values, as well as others not visible in the Field Value panel:

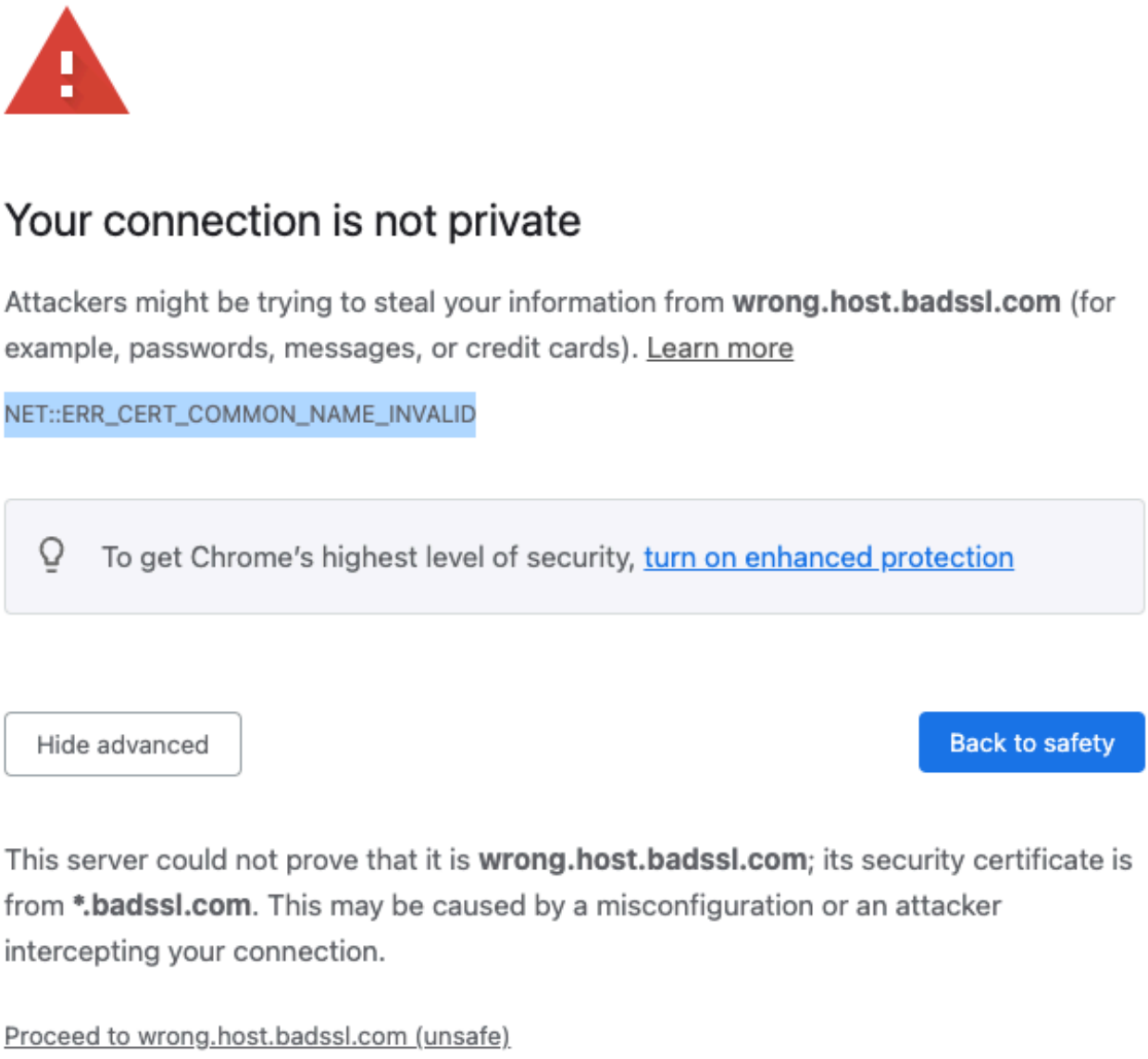
- www.example.org
- example.net

- example.edu
- example.com
- example.org

Note that the SAN "example.com" does not match an SNI of "www.example.com". However, a wildcard SAN of "*.example.com" would match an SNI of "www.example.com", or any other domain name containing a single label (a string with no "." character) prepended to example.com, but not multiple labels. For example, "www.hr.example.com" is not matched by "*.example.com" because "www.hr" consists of two labels: "www" and "hr". A single wildcard can only match a single label.

Certificate Identity Errors

When a web client receives a server certificate, if none of the SAN's DNS Names match the SNI from the domain name in the requested URL, then the web client typically displays an error to the user. This image shows Chrome displaying a "NET::ERR_CERT_COMMON_NAME_INVALID" interstitial page.



In the image, the site requested was "https://wrong.host.badssl.com" which does not match any of the SANs. The certificate contains a wildcard SAN DNS Name, "*.badssl.com" whose wildcard can only match a single label such as "host". Additionally, the certificate does not have a SAN DNS Name with the exact value "wrong.host.badssl.com" or a wildcard SAN of "*.host.badssl.com", so the user is presented with this error.

To identify the reason for a certificate identity mismatch, inspect the certificate's SAN DNS Names using the browser's certificate viewing function and compare with the domain name in the requested URL. Alternatively, a tool such as the Qualys SSL Server Test can be used to diagnose a certificate identity issue.

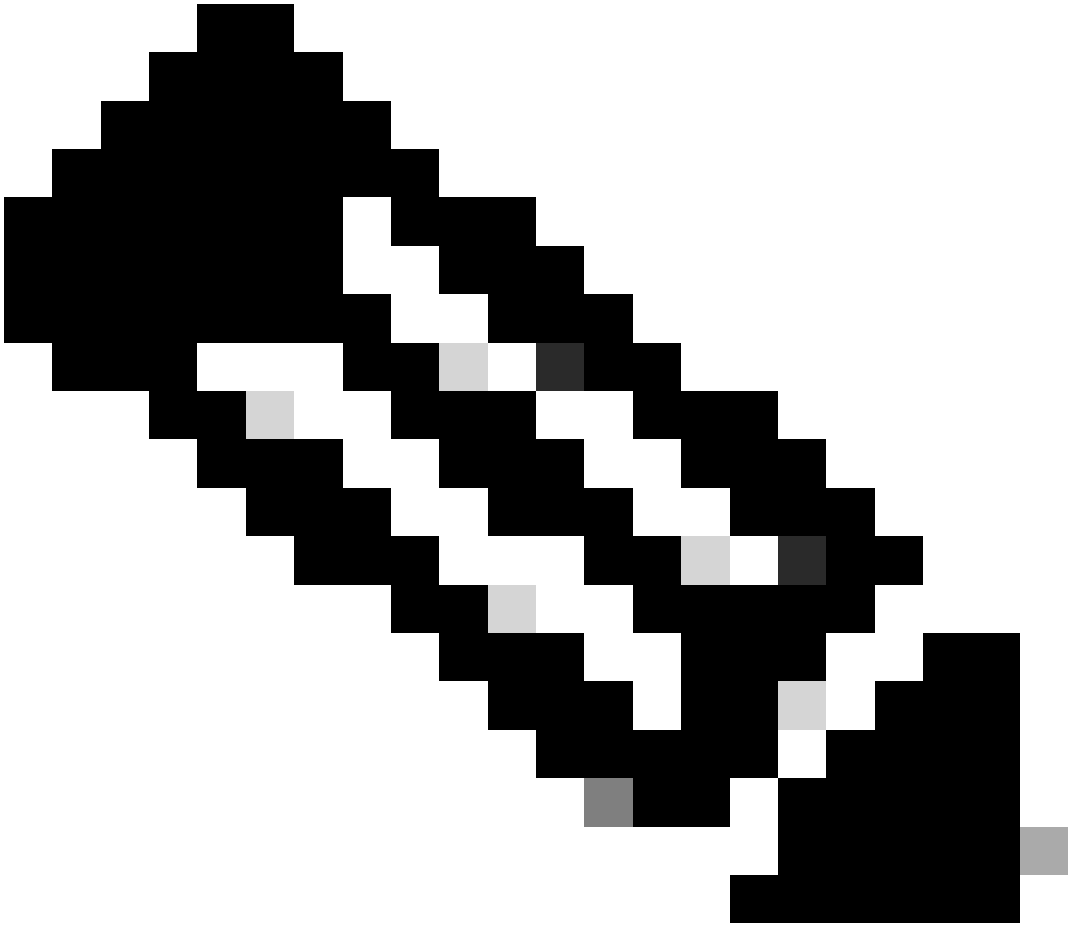
If the reason for the 516 error cannot be identified after employing the information in this section, or if the resolutions and workarounds in the next section cannot be employed, please open a case with Umbrella technical support and provide:

1. a screenshot that captures
    - the browser's address bar showing the requested URL
    - the entire 516 error page (see image in the next section)
2. the text of the URL copied from the address bar

Resolution

To resolve this issue, access the server with a domain name that matches one of the SAN DNS Names in the certificate. This can require the website's administrator to add a matching domain name into the DNS for the zone. Alternatively, the administrator can re-issue the certificate to include the URL's domain name in one of the SAN DNS Names.

As a workaround, the URL's domain name can be added to a Selective Decryption List for the Secure Web Gateway proxy or to a Destination List in the Intelligent Proxy. Apply the list to the appropriate Web policy Ruleset Setting (Secure Web Gateway) or DNS policy Allow List (Intelligent Proxy). This prevents the request to the website from being decrypted by the proxy, which prevents the proxy from displaying a 516 error page.

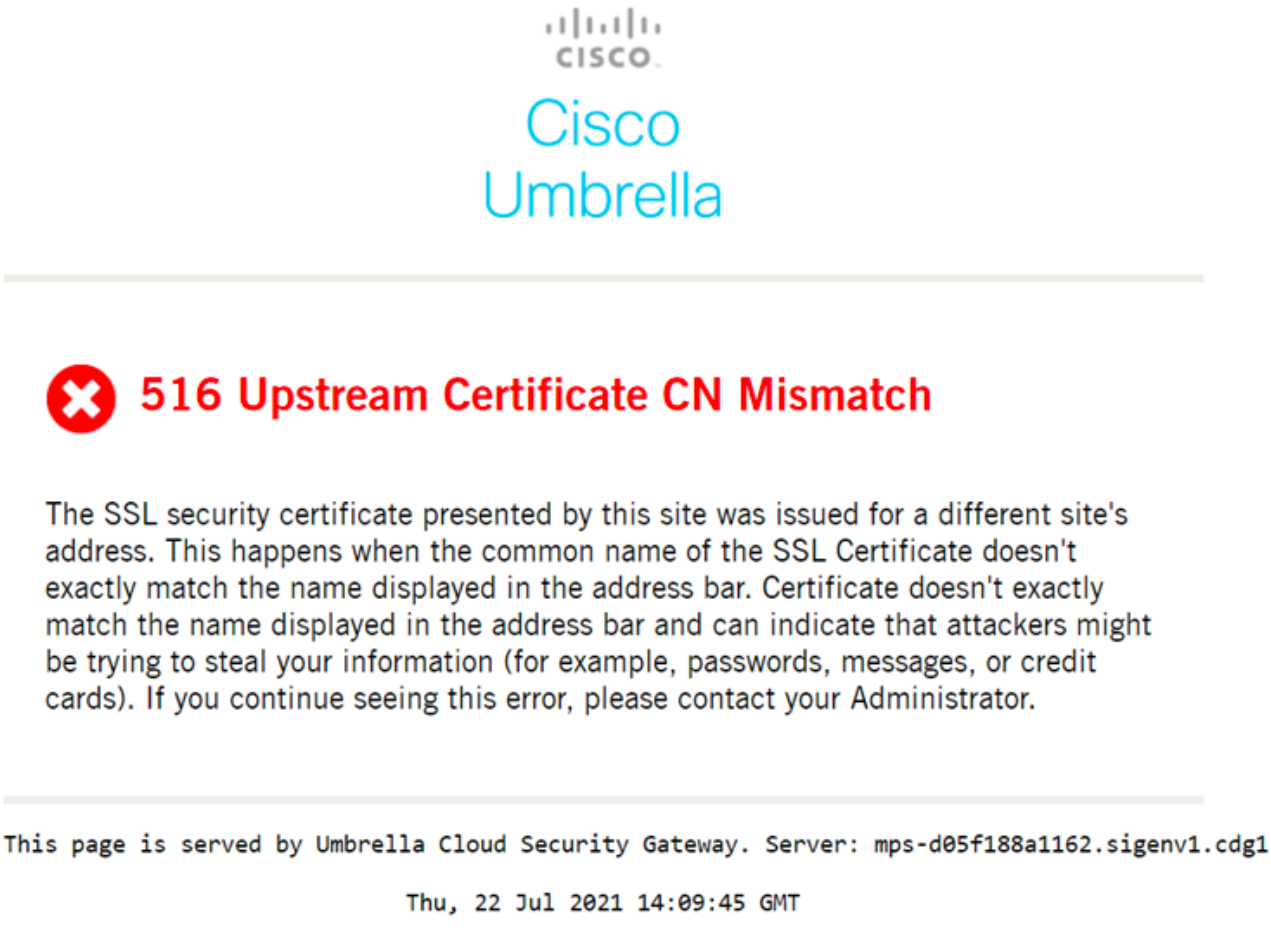


Note: Use of both the Secure Web Gateway proxy and Intelligent Proxy is unsupported. Only one proxy technology can be employed per organization. It is recommended that organizations which have subscriptions for Secure Web Gateway use SWG and not use Intelligent Proxy.

Common Name is Deprecated

Web clients originally matched the domain name in the requested URL to the **Common Name** (CN) attribute in the certificate's **Subject** field. This mechanism has been deprecated in modern web clients; domains are now matched against the **Subject Alternative Name** extension's **DNS Names**. However, text of error messages often continue to reference the deprecated mechanism, such as "NET::ERR_CERT_COMMON_NAME_INVALID" in Chrome.

Similarly, Umbrella SWG displays a 516 error page with this text when the SWG proxy requests a URL from a web server, and a SAN DNS Name mismatch occurs:



16794325789332

Cisco Umbrella plans to update this text at a future date to better reflect the current behavior.

Additional Information

See *RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Section 4.1.2.6 for information on certificate Subject, and Section 4.2.1.6 for information on Subject Alternative Name.