Troubleshoot Umbrella Root Certificate Errors when Using Chrome on Windows

Contents

Introduction

This document describes how to troubleshoot and resolve Umbrella root certificate errors for *cisco.com when using Chrome on Windows.

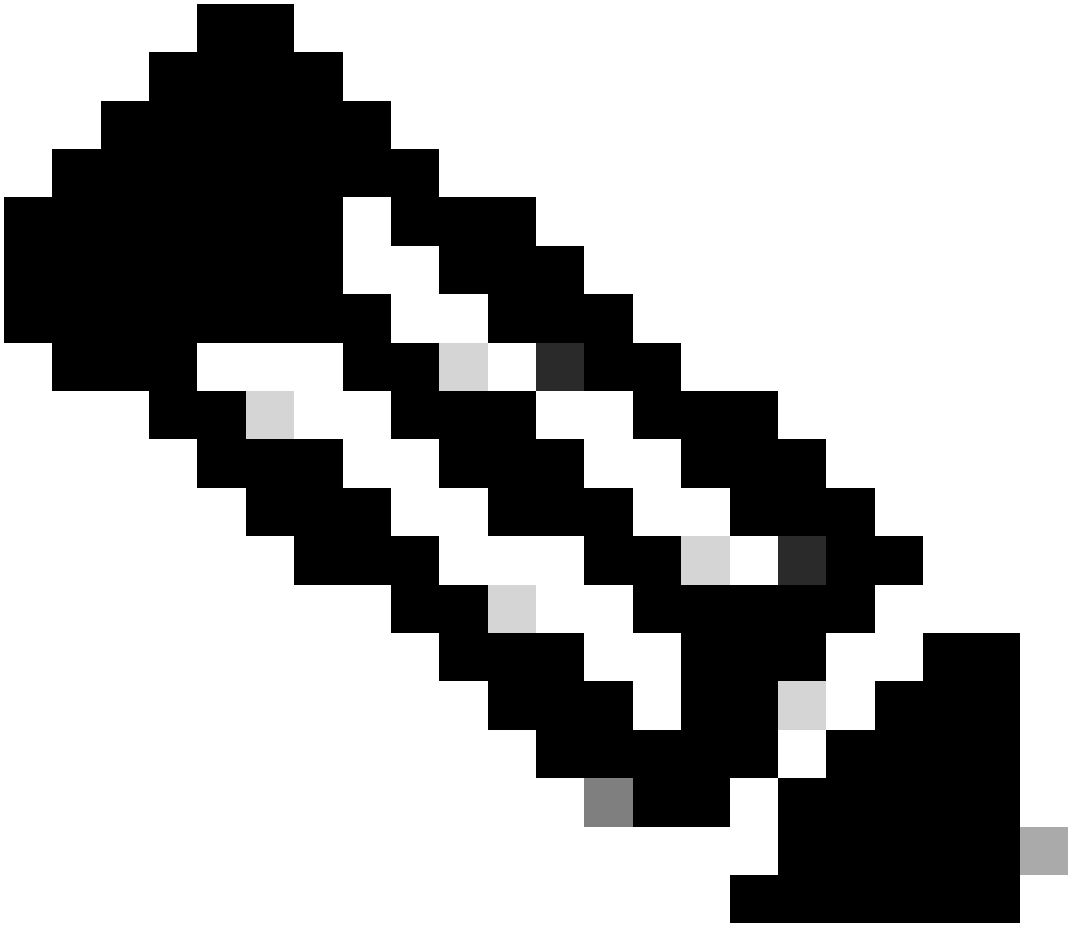
Overview

We now have a more manageable and enduring solution for this issue that applies to all sites. While the information provided here remains relevant, we suggest exploring the permanent fix by installing the Cisco Root CA, as detailed in this article:

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

This page is a guide for when a certificate error for *.cisco.com appears in Chrome (for Windows), but it is not able to be bypassed by adding a certificate exception.

The cause of this message is the implementation of HTTP Strict Transport Security (HSTS) or pre-loaded Certificate Pinning in modern browsers which enhances their overall security. 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. For more information about HSTS, please refer to this article.



Note: Due to changes in HSTS, the Block Page Bypass (BPB) system does not work with certain sites due to non-bypassable certificate errors. In order to allow these sites to work with BPB in Chrome (for Windows), you must use a special switch when starting the browser. Some common sites that do not work with BPBin Chrome include: Facebook, Google Sites such as Gmail and YouTube, Dropbox and Twitter. For a full list of sites, please read here.

Without disabling Chrome Certificate Checks, attempts to use Block Page Bypass with any of the sites on this protected list fail, as shown.

Disabling Chrome Certificate Checks (Windows Only)

To force Chrome to ignore these errors, you need to set your shortcut for Chrome to launch the application with this switch:

```
--ignore-certificate-errors
```

Note that Google can choose to remove this feature at any time and thus it is only recommended as long as it is available:

To add this command line flag to Chrome, right-click the Chrome icon shortcut, select "Properties" and add it to the and selecting "Properties", then adding it to the Target as shown here:

Once this flag is added, you can use BPB normally on the sites in the pre-loaded HSTS list to be able to bypass them.

In this example, although twitter.com is on the HSTS preloaded list, by ignoring the certificate warning we can use Block Page Bypass as designed.