

Resolve Certificate Errors when Using Blocked Page Bypass

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Problem](#)

[Solution](#)

[Cause](#)

Introduction

This document describes how to resolve certificate errors when using Blocked Pages Bypass in Cisco Umbrella.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

If you are using Block Pages Bypass, it is expected that a HTTPS/HSTS certificate error can be raised.

Solution

To ensure that Bypassed Block Page content shows up properly, please ensure that you [add the Cisco Root CA](#).

Cause

This is the correct and expected behavior. When using Bypass Blocked Pages, Umbrella's servers are acting as a forward proxy allowing only the authenticated user to access the domain. If Umbrella changed the DNS

response, all users on your network are able to access the resource.

The HTTPS certificate error is due to this mechanism. Since Umbrella cannot pretend to be whichever domain you are actually trying to connect to, your browser is simply letting you know that the certificate does not match the destination. This does not normally impact your ability to use a particular website.