Understand Public Key Pinning and Certificate Pinning in Umbrella

Contents

Introduction

This document describes certificate pinning and public key pinning 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.

Overview

Certificate pinning is an Internet security mechanism which allows applications to resist impersonation against HTTPS servers using mis-issued or otherwise fraudulent digital certificates. It does this by associating a server with a defined set of public keys, which can be the only ones trusted for connections to that server. There are two techniques for Certificate Pinning:

- **Public Key Pinning** (PKP RFC7469) is a now obsolete mechanism for triggering certificate pinning in web browsers. Pinned certificates are sent to the browser using HTTP headers.
- **Static Certificate Pinning** is where an application is hard-coded to expect specific certificates or certificate authorities. Some desktop/mobile applications use a static certificate pinning mechanism for additional security.

When these web applications are proxied by Umbrella, the public key provided by Umbrella does not match which causes the application to close the HTTPS connection. Certificate pinning most commonly applies to only desktop/mobile applications because PKP support has been removed by modern web browsers.

Compatibility with Umbrella SWG

Umbrella bypasses known URLs from SSL Decryption to resolve certificate pinning issues in certain circumstances. Table 1 includes applications that have been bypassed globally for all Umbrella customers. Table 1 also includes other applications that were known to use certificate pinning at the time or writing. If you are using any of these applications, you can consider using the methods described later, for the reasons given, to bypass the application from HTTPS inspection. Table 2 provides more detail for the application services covered in table 1.

Other Certificate Pinning Applications

Applications can be bypassed on a per-customer (per-policy) basis to solve certificate pinning problems using Umbrella's Selective Decryption feature. These exceptions can be implemented easily based on domain, application name or category; Umbrella SWG includes a large library of applications in our app database.

In most cases the decision whether to bypass the application rests with the IT Administrator. Adding a Decryption exception is a security trade-off because it prevents security/file inspection of the web content. This is an individual decision depending on the type of application and business need. For example, if the certificate pinning issue only affects a mobile/desktop application the Administrator can choose to add an exception to make the mobile application work or can instead prefer to ask users to use the web version of the application.

This is a table of applications that are either bypassed Globally for Umbrella Customers and no action is required or known to use certificate pinning at the time of writing and not bypassed by Umbrella by default. If you are using the applications which are not bypassed by default, then you can consider using the methods described above, for the reasons given, to bypass the application from HTTPS inspection.

Table 1 - Applications that can use certificate pinning

Application Name	**Cisco Umbrella Coverage**
Adobe Services	Bypassed Globally for Umbrella Customers
Airbnb	Supported by Application Control
Amazon Alexa	Supported by Application Control
Amazon Drive	Supported by Application Control
Amazon Kindle	Supported by Application Control
Amazon Workspaces	Supported by Application Control

Amplitude	Bypassed Globally for Umbrella Customers
App Dynamics	Bypassed Globally for Umbrella Customers
Apple iMessage	Supported by Application Control
Apple Mail	Supported by Application Control
Apple Services *(see **table 2** for more detail)*	Bypassed Globally for Umbrella Customers
Cisco Services *(see **table 2** for more detail)*	Bypassed Globally for Umbrella Customers
Citrix Workspace	Supported by Application Control
Crashlytics	Bypassed Globally for Umbrella Customers
CrowdStrike Falcon	Supported by Application Control
Diligent.com	Supported by Application Control
Discord Chat	Bypassed Globally for Umbrella Customers
DocuSign Agreement Cloud	Supported by Application Control
DropBox	Supported by Application Control
Druva Cloud Backup	Supported by Application Control
Egnyte Connect	Supported by Application Control
Evernote	Supported by Application Control
Facebook Messenger	Supported by Application Control
Facebook	Supported by Application Control
Filemail	Supported by Application Control

Foursquare	Supported by Application Control
Giphy	Bypassed Globally for Umbrella Customers
GitHub	Supported by Application Control
Google Drive	Supported by Application Control
Google Play Store	Supported by Application Control
Google Services *(see **table 2** for more detail)*	Bypassed Globally for Umbrella Customers
Google Workspace	Supported by Application Control
GoToMeeting	Supported by Application Control
Hype Machine	Supported by Application Control
Instagram	Supported by Application Control
LogMein Pro	Supported by Application Control
Microsoft Defender for Endpoint	Supported by Application Control
Microsoft Intune	Supported by Application Control
Microsoft Services *(see **table 2** for more detail)*	Bypassed Globally for Umbrella Customers
Microsoft Xbox Live	Supported by Application Control
Netflix	Supported by Application Control
OpenDrive	Supported by Application Control
PayPal	Supported by Application Control
PingOne Identity	Supported by Application Control

Rackspace / Cloud Drive Services	Bypassed Globally for Umbrella Customers
Salesforce CRM	Supported by Application Control
Segment	Bypassed Globally for Umbrella Customers
Signal Platform	Supported by Application Control
Skype for Business	Supported by Application Control
Snapchat	Supported by Application Control
Soundcloud	Supported by Application Control
SpiderOak	Supported by Application Control
Spotify	Supported by Application Control
TeamViewer	Supported by Application Control
TikTok	Supported by Application Control
Todoist	Supported by Application Control
Twitter	Supported by Application Control
Vimeo	Supported by Application Control
Workday HCM	Supported by Application Control
Zoom Meetings	Bypassed Globally for Umbrella Customers

Table 2 – Detail forServices bypassed globally as shown in table 1

Apple Services	• Apple Captive Portal Check • Apple iTunes and App Store • Additional Apple platform services

Cisco Services	• Cisco Umbrella & OpenDNS Services • Cisco Webex & Webex Teams • Cisco Cloud Email Security WebUI • AMP endpoint service • Duo Security 2FA
Google Services	• Google Hangouts • Google Messages on web • Additional Google platform services
Microsoft Services	• Microsoft Network Connectivity Status Indicator • Windows Update • Windows translation service • Additional Microsoft / Windows platform services

For additional help, please see Troubleshooting Non-Browser Applications or contact Umbrella Support. Applications may be considered for addition to our global bypass list after they have been reviewed by the Engineering team.