iOS SSL Certificate Installation

Version 1.3.0

August 2017

Introduction

This document describes how to get the Cato SSL Certificate and deploy it locally on **iOS** devices.

Overview

Installing the Cato Networks Certificate, and adding it as a trusted application, allows users to benefit from Cato security services and reduce the extra system notifications produced by the following instances:

- **Block HTTPS traffic:** If SSL traffic is being blocked (i.e. URL filtering, Internet Firewall rules), Cato Network Certificate allows access to blocked pages.
- **TLS inspection on client's traffic:** If TLS is enabled, the web browser prompts that the connection is not private (as expected certificate was supposed to be issued by the target). The Cato Network Certificate bypasses this notification.
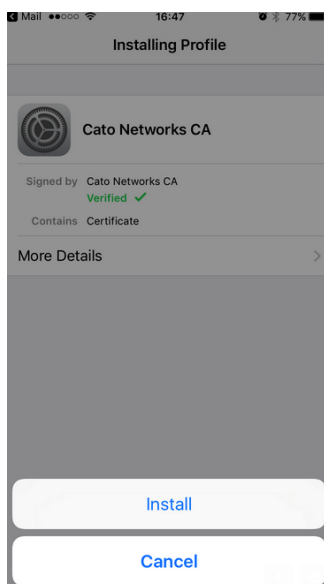
Installing on iOS

1. Open the relevant CER file
   Note: You must use the Safari browser to download and open the certificate, or use the apple mail client (if you have received the cert file via and email)

2. The Install Profile popup opens. Press **Install**.

3. Press **Install** again.

4. Upon completion of the installation process, press **Done**

5. (iOS 10.3 and later) Go to Settings > General > About > Certificate Trust Settings. Under "Enable full trust for root certificates," **turn on** trust for the Cato Networks CA certificate.

Installing on FireFox

If Firefox is the browser on your device, execute the following steps to install the Cato Networks Certificate:

1. Go to Options>Advanced>Certificates.
2. Press "**View Certificates**".
3. Press "**Import**".
4. Browse to the location where you stored the certificate, select it and press "**Open**".
5. Press "**Import".** In the Downloading Certificate dialog, select "**Trust this CA to identify websites**" and press **OK**.

Additional resources

If additional assistance is needed, please contact Cato Network's support at support@catonetworks.com