CATO NETWORKS

Mac OS SSL Certificate Installation

Version 1.2.1

December 2016

Introduction

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

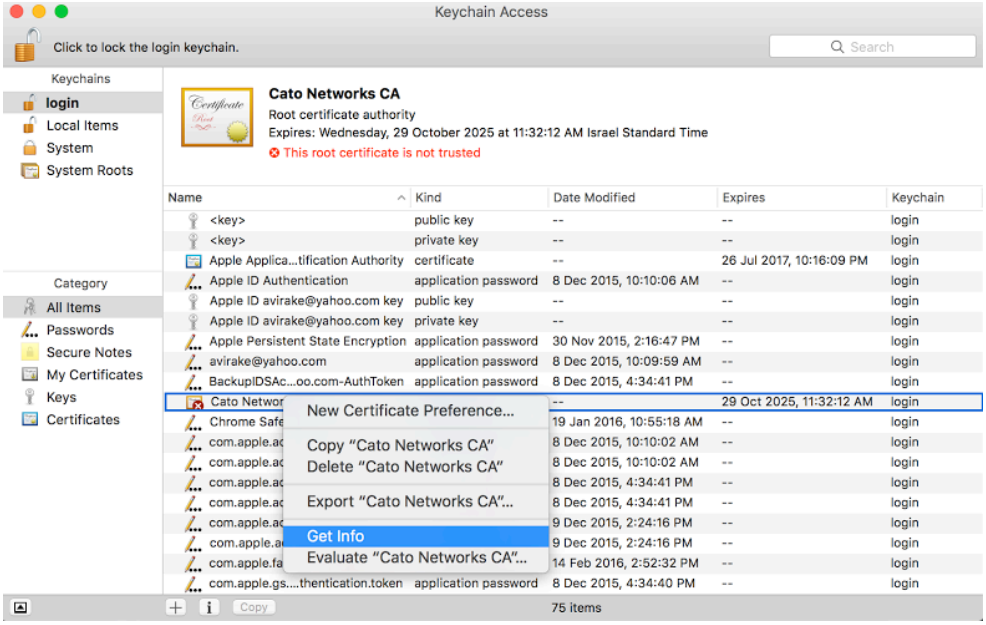
Overview

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:

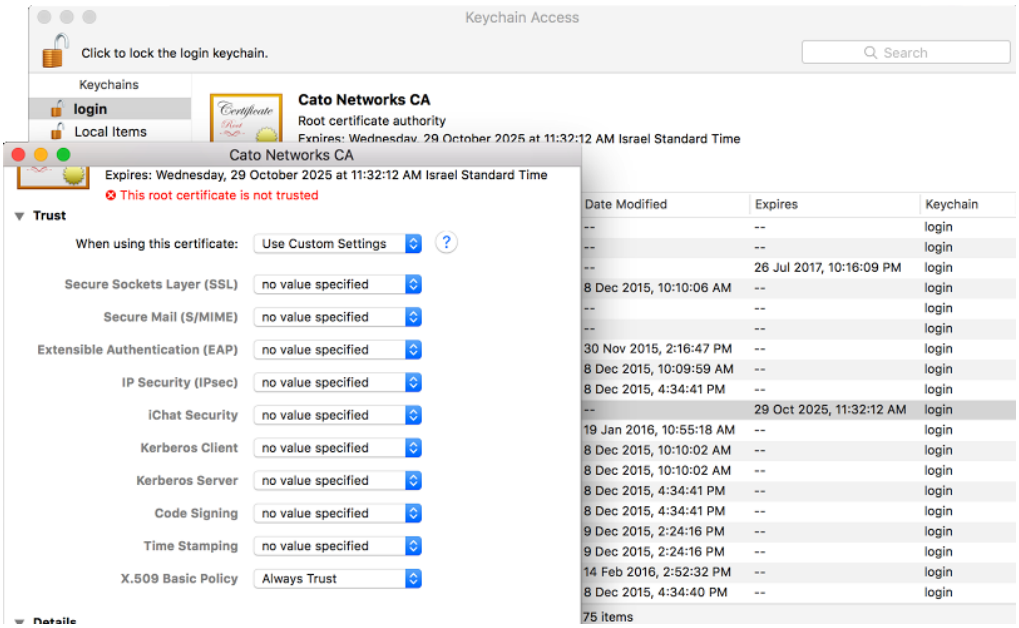
- **Block HTTPS traffic:** If SSL traffic is being blocked (i.e. URL filtering, Internet Firewall rules), Cato Network Certificate allows access to blocked pages.
- **TLS inspection on client's traffic:** If TLS is enabled, the web browser prompts that the connection is not private (as expected certificate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

Installing on macOS

1. Double click the relevant CER file
2. The "Add Certification" message appears. Click **Add**.
3. Open the Keychain Access Manager. Right click **Cato Networks CA** and choose **Get Info**.



4. Expand the "Trust" section and change the **X.509 Basic Policy** parameter to **Always Trust**. Close the popup window.



5. Enter your computer account password and click **Update Settings**.

You have now successfully installed the certificate and configured trust.

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. Click "**View Certificates**".
3. Click "**Import**".
4. Browse to the location where you stored the certificate, select it and click "**Open**".
5. Click "**Import".** In the Downloading Certificate dialog, select "**Trust this CA to identify websites**" and click **OK**.

Additional resources

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