SSL PROXY CERTIFICATION
Installation Guide

Network Box SSL Proxy secures communication between two internet endpoints by decrypting secure connections on the way in, performing security analysis, then re-encrypting data on the way out. Incoming and outgoing SSL connections over the internet are upgraded to use as secure settings as possible, following the approach of highest common denominator security, rather than the lowest. The engine also moves the choice of bypassing failed SSL server certificate validation away from the end-user and to the IT Manager.

To install, please follow the appropriate step(s), for the platform you are using:

WINDOWS

(Internet Explorer / Chrome and other applications)

1. Import the HTTPS proxy CA certificate file.
2. Open the Microsoft Management Console (mmc). Click on the **File** menu and then Add/Remove Snap-in.
   The Add or Remove Snap-ins dialog window opens.
3. Click **Add** at the bottom of the window.
   The dialog window Add Standalone Snap-In opens.
4. Select Certificates from the list and click **Add**.
5. Select Computer account and click **Next**.
6. The Console Root now contains the item Certificates (Local Computer).
7. In the Console Root window on the left open Certificates > Trusted Root Certification Authorities, right-click **Certificates** and select All Tasks > Import from the context menu.
   The import dialog wizard opens.
8. Click **Next**.
   The next wizard step is displayed.
9. Browse to the previously downloaded HTTPS proxy CA certificate(xxx.crt), click **Open** and then **Next**.
   The next wizard step is displayed.
10. Make sure that Place all certificates in the following store is selected and click **Next** and **Close**.
    The wizard reports the import success.
11. Confirm the installation wizard's message.
    The proxy CA certificate is now displayed among the trusted certificates.

Mac OS

(Safari / Chrome and other applications):

1. Import the HTTPS proxy CA certificate file.
2. Double-click to open the file.
   The Keychain Access window will pop-up
3. In the window, the CA certificate file will be highlighted. Click **Always Trust**.
4. Enter your user name and password for authentication, and click **OK**.
   The certificate should now be installed.

FIREFOX

Firefox has its own CA store, you will need to add it individually.

1. Open Firefox, go to Options.
2. Select Certificates from Advanced tab.
3. Click **View Certificates**.
4. Go to Authorities tab and click Import. Browse to the previously downloaded HTTPS proxy CA certificate(xxx.crt), click **Open**.
5. Check the check-box Trust this CA to identify websites, click **OK**.

iOS

1. You will receive an HTTPS proxy CA certificate(xxx.crt) file from the administrator.
2. Open the file, press **Install**.
3. Enter your iphone/ipad passcode, press **Install**.
4. The installation wizard will report that the installation has been successful.

Andriod

This is for Android version 4.4.4.
The procedure may differ slightly depending on the version.

1. You will receive an HTTPS proxy CA certificate(xxx.crt) file from the administrator,

2. Open the file, press **install**.

OR, if you have the file copied onto an SD card
Settings > Security > Install from SD card

3. Name the certificate

4. To check if it has been installed, go to Settings > Security > Trusted Credentials > USER.
The certificate should appear here.