Adding Trusted Root Certificates to the Ser

Author: Luis Fernandes 2 years ago

Overview

A trusted root certificate must be added manually if you want to send or receive messages signed by root au
installed on the server.

Step-By-Step Guide

Mac OS X

1. To add, use the command:
   sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain ~/new-root-certifi

2. To remove, use the command:
   sudo security delete-certificate -c "<name of existing certificate>"

Windows

1. To add, use the command:
   certutil -addstore -f "ROOT" new-root-certificate.crt

2. To remove, use the command:
   certutil -delstore "ROOT" serial-number-hex

Linux (Ubuntu, Debian)

1. To add:
   1. Copy your CA to `dir /usr/local/share/ca-certificates/`
   2. Use command: `sudo cp foo.crt /usr/local/share/ca-certificates/foo.crt`
   3. Update the CA store: `sudo update-ca-certificates`
2. To remove:
   1. Remove your CA.
   2. Update the CA store: `sudo update-ca-certificates --fresh`

Note: Restart Kerio Connect to reload the certificates in the 32-bit versions or Debian 7.

Linux (CentOs 6)

To add:

1. Install the ca-certificates package: `yum install ca-certificates`
2. Enable the dynamic CA configuration feature: `update-ca-trust force-enable`