Adding trusted root certificates to the server

If you want to send or receive messages signed by root authorities and these authorities are not installed on the server, you must add a trusted root certificate manually.

Use the following steps to add or remove trusted root certificates to/from a server.

Mac OS X

Function	Method
Add	Use command: `sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain ~/new-root-certificate.crt`
Remove	Use command: `sudo security delete-certificate -c "<name of existing certificate>"`

Windows

Function	Method
Add	Use command: `certutil -addstore -f "ROOT" new-root-certificate.crt`
Remove	Use command: `certutil -delstore "ROOT" serial-number-hex`

Linux (Ubuntu, Debian)

Function	Method
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`

Function	Method
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)

Function	Method
Add	1. Install the ca-certificates package: `yum install ca-certificates` 2. Enable the dynamic CA configuration feature: `update-ca-trust force-enable` 3. Add it as a new file to /etc/pki/ca-trust/source/anchors/: `cp foo.crt /etc/pki/ca-trust/source/anchors/` 4. Use command: `update-ca-trust extract`

> **NOTE**
> Restart Kerio Connect to reload the certificates in the 32-bit version.

Linux (CentOs 5)

Function	Method
Add	Append your trusted certificate to file /etc/pki/tls/certs/ca-bundle.crt `cat foo.crt >>/etc/pki/tls/certs/ca-bundle.crt`

> **NOTE**
> Restart Kerio Connect to reload the certificates in the 32-bit version.