



Installation Guide

Version 5.5



Security Hint: Do **not import** the common CA Root Certificate delivered by the ZebraTester installation kit (file: **root.cer**) into your OS or into your Web browser. You have to create your own CA Root Certificate.

Table of Contents

1	Installation	3
1.1	System Requirements	3
1.2	Recommendations for Load Generators (Exec Agents)	3
1.3	Installation on Windows	4
1.3.1	Generating an own, private CA Root Certificate on Windows	6
1.3.2	Windows System Tuning	12
1.3.2.1	Disabling HTTP/S Anti-Virus Network-Scanning	14
1.3.3	Further Hints for using ZebraTester on Windows - Firefox Portable and Firefox Recording Extension	15
1.4	Installation on Mac OS X / macOS	17
1.4.1	Generating an own, private CA Root Certificate on Mac OS X / macOS	21
1.4.2	Mac OS X / macOS System Tuning	26
1.4.3	Using a Public JDK on Mac OS X / macOS	28
1.5	Installation on Linux	29
1.5.1	Generating an own, private CA Root Certificate on Linux	35
1.5.2	Linux Tuning	38
1.6	Manual Installation on all Unix-like Systems (Linux, Solaris, BSD, Mac OS X ...)	39
1.6.1	Generating an own, private CA Root Certificate on Unix-Like Systems	40
2	Architecture Overview	42
2.1.1	Local Architecture	42
2.1.2	Distributed Architecture	43
2.1.2.1	Configuring Additional Load Generators (Exec Agents)	44
2.2	Protecting the Web Admin GUI from Unauthorized Remote Access	45
2.2.1	Enabling the Remote Access Protection	45
3	Reconfiguring the Web Browser for the Recording of Web Surfing Sessions	49
3.1	Enabling Pop-up Windows from Local Host	50
3.2	Reconfiguring a Web Browser for Recording	53
3.2.1	Microsoft Internet Explorer Proxy Configuration	54
3.2.2	Firefox Proxy Configuration	55
3.2.3	Google Chrome Proxy Configuration	56
3.2.4	Safari Proxy Configuration	57
3.3	Clearing the Web Browser Cache and all Cookies every time before Recording	58
3.3.1	Internet Explorer / Clearing Cache and Cookies	58
3.3.2	Firefox / Clearing Cache and Cookies	59
3.3.3	Google Chrome / Clearing Cache and Cookies	60
3.3.4	Safari / Clearing Cache and Cookies	61
3.4	Recording via an Outbound Proxy Server of your Company	62
	Appendix A: Import your CA Root Certificate into an Apple iOS device (iPhone and iPad)	63

1 Installation

Normally, administrator rights are **not required** when installing ZebraTester in the suggested default location.

In addition, after installation, ZebraTester requires write access to its own installation directory and to the associated sub-directories.

1.1 System Requirements

- Supported operating systems: **Windows XP/7/8/10/2008/2013, Mac OS X / macOS, Linux, Solaris.**
- **RAM: 4096 MB** recommended, minimum **2048 MB**.
Note: The Windows 64-Bit installation kit for high-duty load generators requires at minimum 16 GB RAM, 24 GB RAM recommended.
- **Display** (Web GUI): Minimum recommended screen resolution: **1280 x 800 pixels**.
- **Disk Space**: Minimum **500 MB free**.
- On Linux and Solaris (only): A Java SDK (Java Software Development Kit) 1.7 (Java version 7) must be pre-installed ¹
- Adobe Reader or Foxit Reader to display PDF files.

¹ On **Linux and Solaris**: The successful operation of ZebraTester requires that you pre-install the original SDK implementation from Oracle (Java 1.7 only) – all other SDK implementations are not supported.

For **Windows and Mac OS X / macOS** systems: No pre-installation required. An own Java 1.7 compiler and interpreter is already bundled with the ZebraTester installation kit. The installed Java SDK of ZebraTester does not tamper any other Java installations on your machine.

Do not install the Windows 64-Bit installation kit if your machine has less than 16 GB of RAM. In such a case install always the Windows 32-Bit installation kit of ZebraTester, even if your machine runs with Windows 64-Bit.

1.2 Recommendations for Load Generators (Exec Agents)

We recommend to use always 64-Bit operating systems for Load Generators (for example Linux-Ubuntu, Solaris or Windows 2013) and to use/install the official **JAVA 1.7 (Java 7) 64-Bit version of the Java SDK from Oracle**.

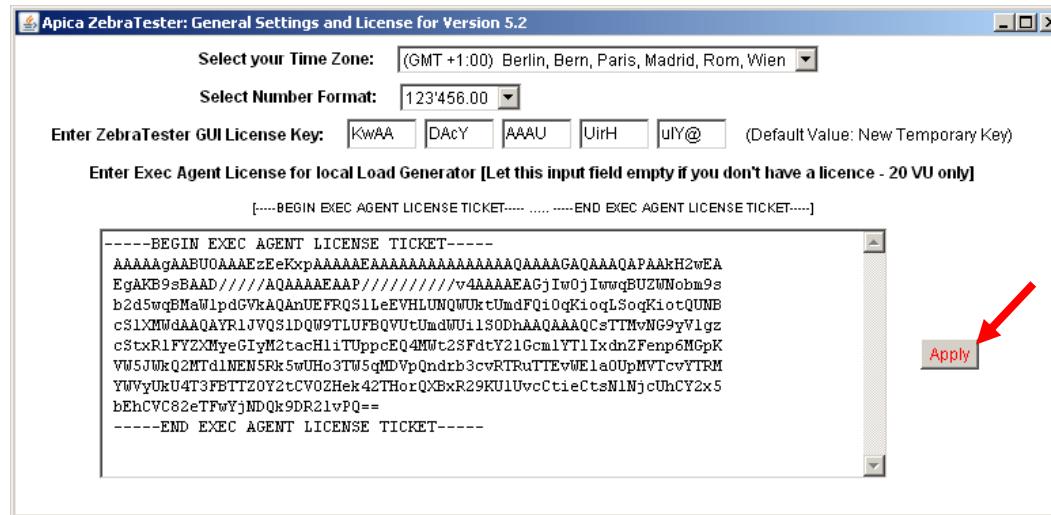
If you run load generators on **Windows Systems** we recommend that you **reconfigure the Virus Scanner in such a way that the HTTP(S) network traffic is not scanned for viruses**. Scanning for viruses on disk (reading and writing of files) and scanning for viruses in emails should still be enabled.

Combinations of heterogeneous operating systems are supported. For example, the ZebraTester GUI (Controller) can be installed/operated on a Mac OS X system and the Exec Agents (Load Generators) be installed/operated on Linux systems.

1.3 Installation on Windows

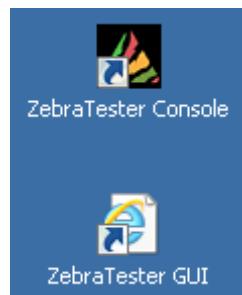
Start **ZBA55<minor version>.exe** and follow the installation instructions. If you accept the suggested default settings you don't require administrator rights. In combination with installing the Firefox Portable web browser (see chapter [1.3.3](#)) no administrator rights are required to use all functionality of the ZebraTester product.

During the installation you must enter (or review) your license data. **Note that you must click on the Apply button** in order that the new license is stored on disk:



Note: If you install only the GUI component of ZebraTester, enter only the "GUI License Key" but no "Exec Agent License Ticket". On the other hand, if you install only a load generator without GUI, enter only the "Exec Agent License Ticket" but no "GUI License Key".

If you purchased a license for a load generator you can start the load generator also as a Windows Service. In such a case you have first to disable Windows UAC. After that run the batch file `InstallExecAgentService.bat`, respectively `InstallExecAgentServiceWin64.bat`. These files are located in the ZebraTester installation directory.



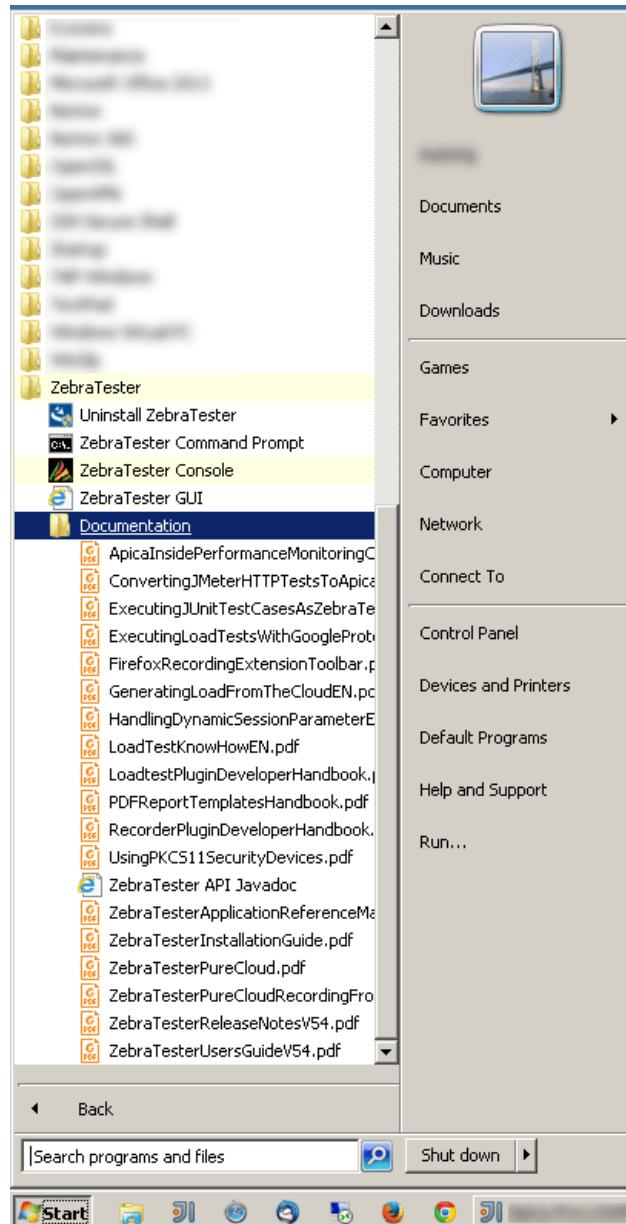
After installation, 2 new icons are placed on the desktop, and new entries are created in the **Start ▶ All Programs ▶ ZebraTester** menu.

If you wish, you can delete these 2 desktop icons – the same icons can also be called from the start menu.

Security Hint: If you install ZebraTester the first time on a Windows system it's strongly recommended that you create your own CA Root Certificate → see next chapter.

Start ZebraTester by clicking first on the **ZebraTester Console** icon, and then by clicking on the **ZebraTester GUI** icon.

Start ▶ All Programs ▶ ZebraTester ▶ Documentation contains also the full product documentation:



1.3.1 Generating an own, private CA Root Certificate on Windows

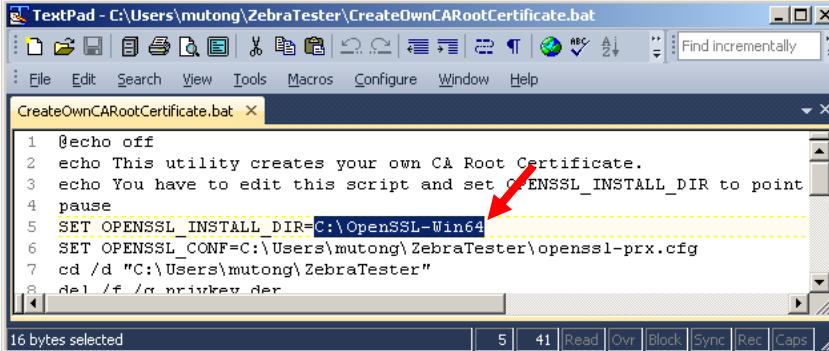
If you install ZebraTester the first time on a Windows system **it's strongly recommended that you create your own CA Root Certificate**. Proceed as follows:

1. Download and install **OpenSSL** for Windows from <http://slproweb.com/products/Win32OpenSSL.html>

We recommend that you select "**Win32 OpenSSL v1.0.1c**" (or a newer version). During installation ignore any warnings of OpenSSL. OpenSSL is needed only to generate the CA Root Certificate. You may also share the CA Root Certificate (root.cer) and its private key (privkey.der) with other members of your team.

2. **Edit** the file **CreateOwnCARootCertificate.bat** which is located in the ZebraTester installation directory (typically at C:\Users\<your-name>\ZebraTester).

Modify the value for **OPENSSL_INSTALL_DIR** to point to your OpenSSL installation directory:

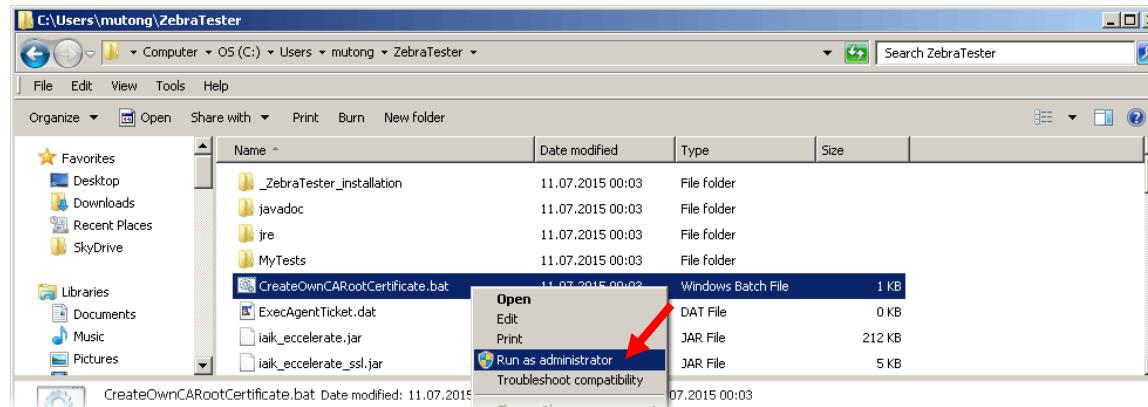


```

1 @echo off
2 echo This utility creates your own CA Root Certificate.
3 echo You have to edit this script and set OPENSSL_INSTALL_DIR to point
4 pause
5 SET OPENSSL_INSTALL_DIR=C:\OpenSSL-Win64
6 SET OPENSSL_CONF=C:\Users\mutong\ZebraTester\openssl-prx.cfg
7 cd /d "C:\Users\mutong\ZebraTester"
8 del /f /a privkey.der

```

3. Execute **CreateOwnCARootCertificate.bat** – as far as possible with Administrator rights:



4. Enter any obvious input for your private CA Root Certificate:

```
This utility creates your own CA Root Certificate.  
You have to edit this script and set OPENSSL_INSTALL_DIR to point to your OpenSSL installation directory.  
Press any key to continue . . .  
Loading 'screen' into random state - done  
Generating a 2048 bit RSA private key  
.....+++  
.....+++  
writing new private key to 'privkey.pem'  
----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
----  
Organization Name (company) [My Company]:My Company  
Organizational Unit Name (department, division) []:Load Testing Team  
Email Address []:direct@d-fischer.com  
Locality Name (city, district) [My Town]:Langenthal  
State or Province Name (full name) [State or Providence]:Bern  
Country Name (2 letter code) [US]:CH  
Common Name (hostname, IP, or CA name) []:ZebraTester Root Certificate (Karl Smith)  
Deleting old Web server certificates ...  
Could Not Find C:\Users\mutong\ZebraTester\*.crt  
Could Not Find C:\Users\mutong\ZebraTester\*.privkey  
Volume in drive C is OS  
Volume Serial Number is 6417-67CC  
Directory of C:\Users\mutong\ZebraTester  
11.07.2015 01:04           1'217 privkey.der  
1 File(s)           1'217 bytes  
0 Dir(s)  376'909'885'440 bytes free  
Volume in drive C is OS  
Volume Serial Number is 6417-67CC  
Directory of C:\Users\mutong\ZebraTester  
11.07.2015 01:04           1'814 root.cer  
1 File(s)           1'814 bytes  
0 Dir(s)  376'909'885'440 bytes free  
---  
Your CA Root Certificate is now created and can be imported into Windows and into Firefox.  
Restart ZebraTester to take effect.  
Press any key to continue . . .
```

5. Restart the ZebraTester Console and verify your CA Root Certificate using the Web Admin GUI:

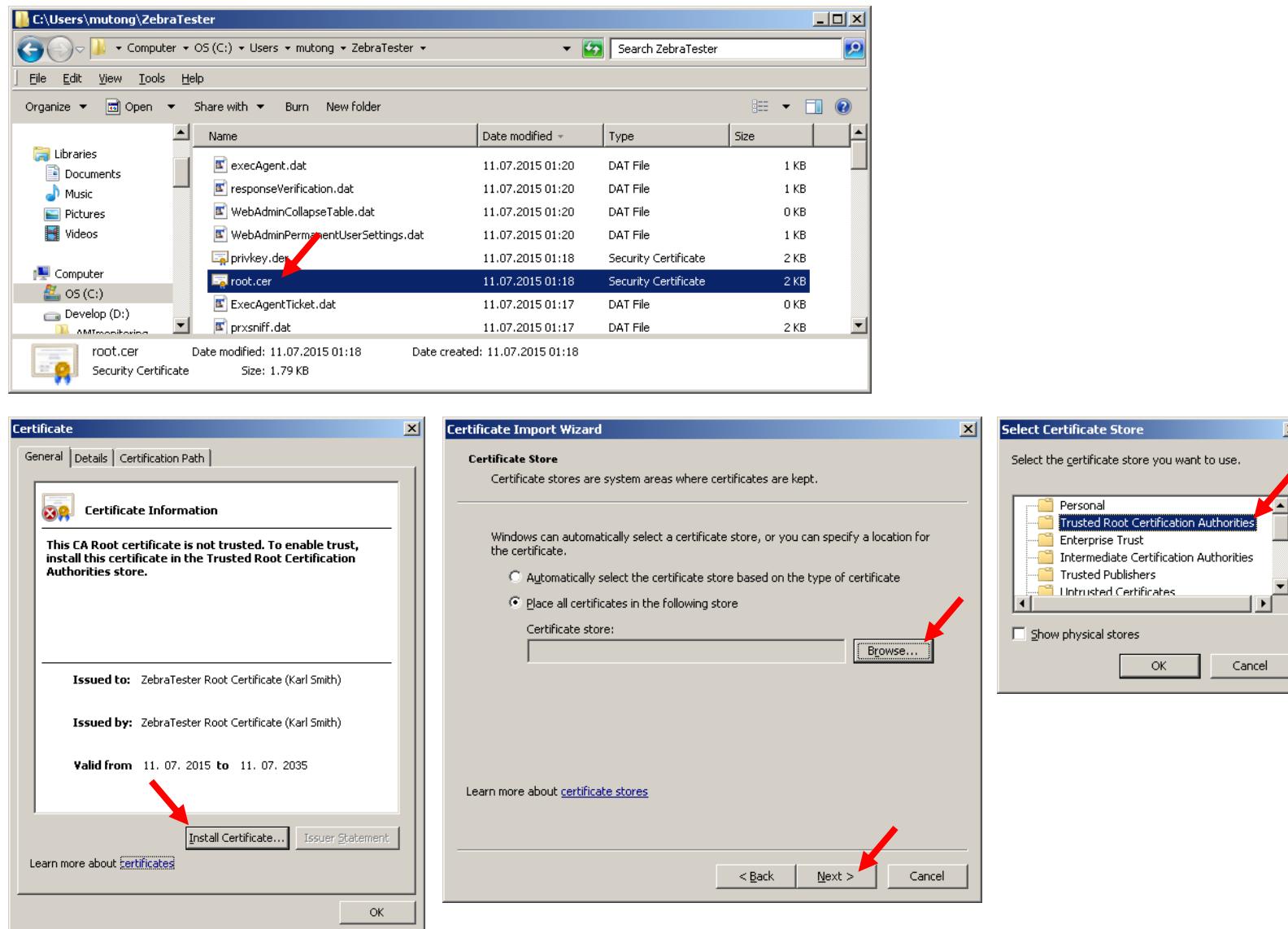
The screenshot shows two windows from the ZebraTester Web Admin interface. The top window is titled 'Main Menu' and has a red arrow pointing to the 'Web Admin V5.2-V' link in the top left corner. The bottom window is titled 'CA Root Certificate - Used for Recording HTTPS Sessions'. It displays the certificate details for 'CN=ZebraTester Root Certificate (Karl Smith)'. The Issuer information is highlighted with a red box: 'Issuer: CN=ZebraTester Root Certificate (Karl Smith), C=CH, ST=Bern, L=Langenthal, EMAIL=direct@d-fischer.com, OU=Load Testing Team, O=My Company'. Other visible details include the Subject, RSA public key, modulus, and certificate fingerprints.

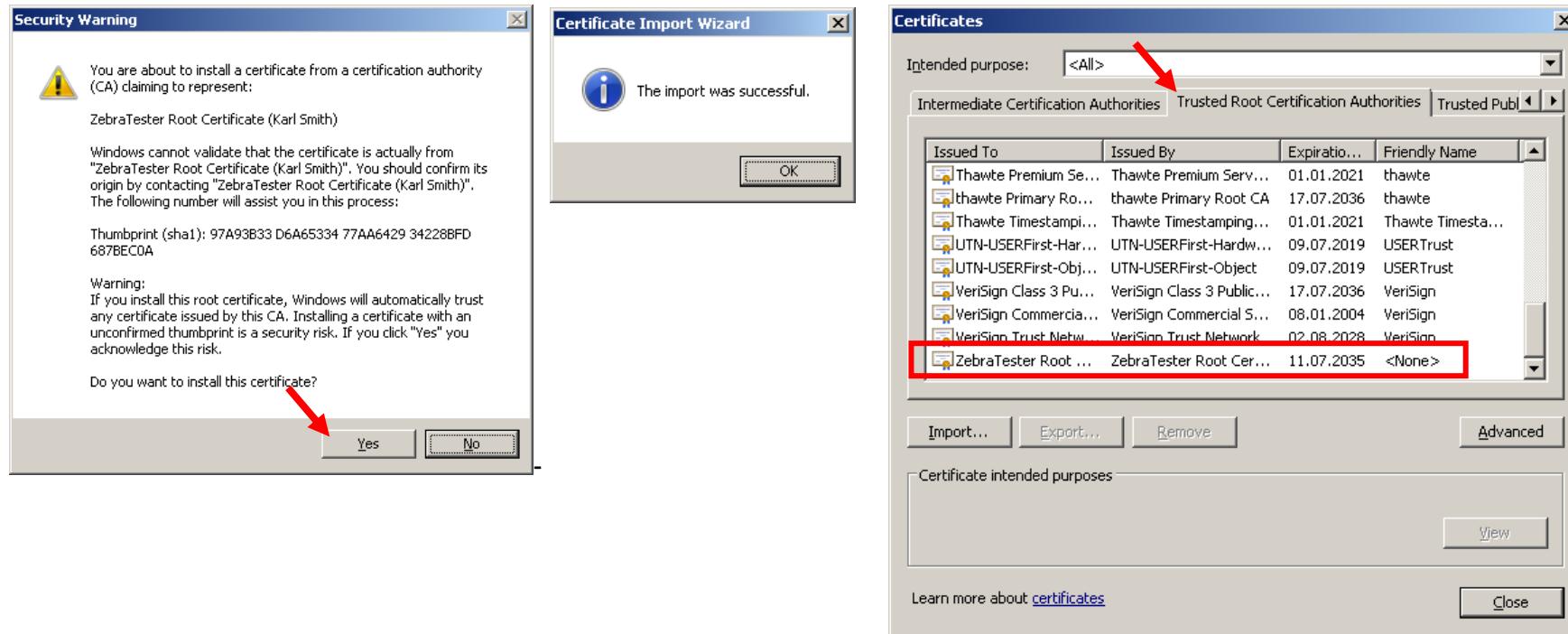
CA Root Certificate: Used to create all faked Web Server Certificates when recording encrypted HTTPS Sessions:
File: C:\Users\mutong\ZebraTester\root.cer

Version: 3
Serial number: 16975497928779405853
Signature algorithm: sha1WithRSAEncryption (1.2.840.113549.1.1.5)
Issuer: CN=ZebraTester Root Certificate (Karl Smith), C=CH, ST=Bern, L=Langenthal, EMAIL=direct@d-fischer.com, OU=Load Testing Team, O=My Company
valid not before: Sat Jul 11 01:18:22 CEST 2015
not after: Wed Jul 11 01:18:22 CEST 2035
Subject: CN=ZebraTester Root Certificate (Karl Smith), C=CH, ST=Bern, L=Langenthal, EMAIL=direct@d-fischer.com, OU=Load Testing Team, O=My Company
RSA public key (2048 bits):
public exponent: 10001
modulus: b64df7ebfb8f08c088499cc17073e13dee225019e02342d64f95bc3cec145a58b3e517d53d2ce1d5c4c37d49388e2c97e8e3af0fe7fbb18ef7a201f4aa9331044afdb6f0c1f9b37156
Certificate Fingerprint (MD5) : 94:DA:E8:9F:B4:A2:9F:02:18:95:53:FE:D9:B4:F9:80
Certificate Fingerprint (SHA-1): 97:A9:3B:33:D6:A6:53:34:77:AA:64:29:34:22:6B:FD:68:7B:EC:0A
Extensions: 3

Private Key for CA Root Certificate:
File: C:\Users\mutong\ZebraTester\privkey.der
[available]

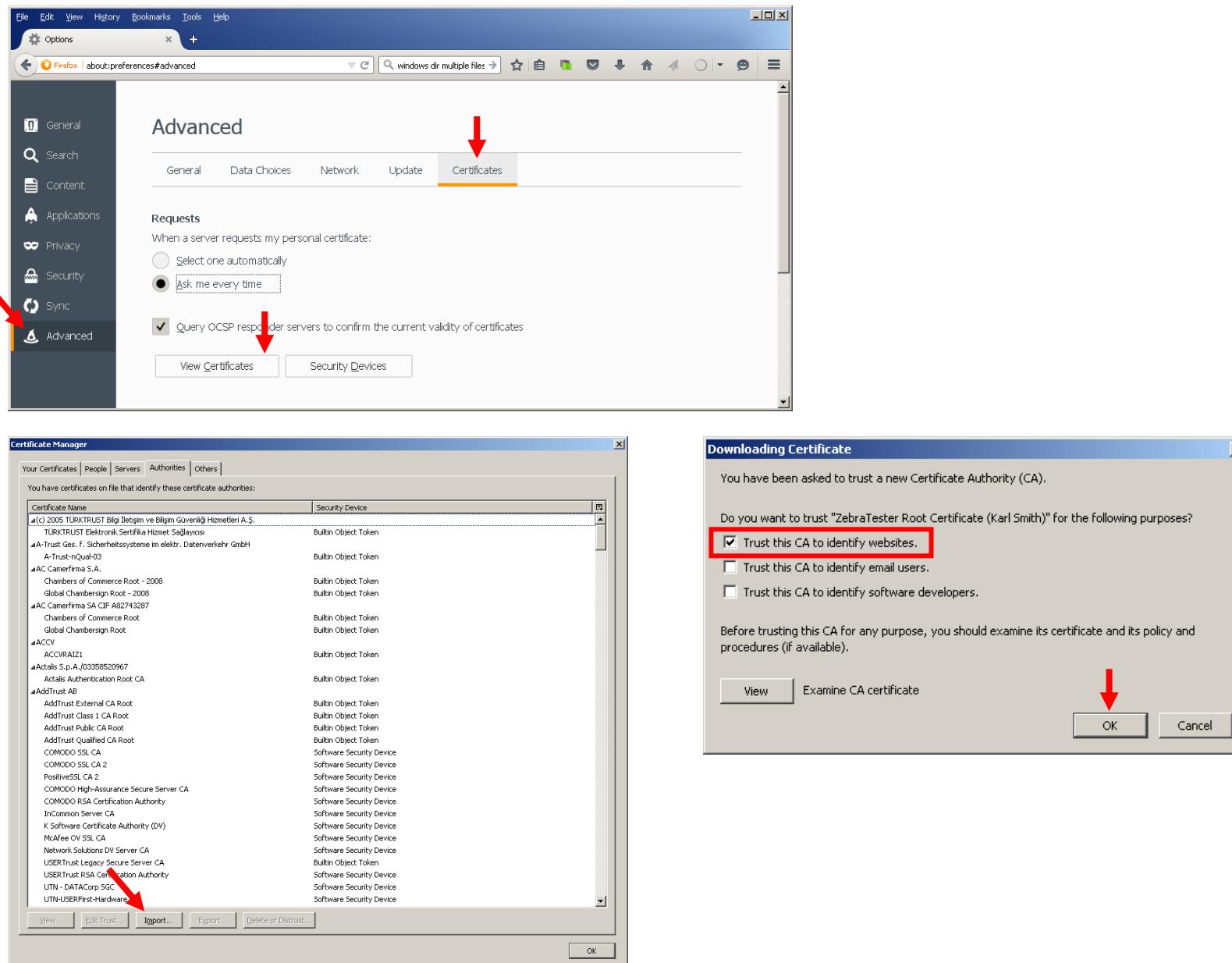
6. Import the CA Root Certificate into Windows. Choose as certificate store **Trusted Root Certificate Authorities**:





Your CA Root Certificate is **listed with the name** as you have entered into the input field "**Common Name (hostname, IP, or CA name)**".

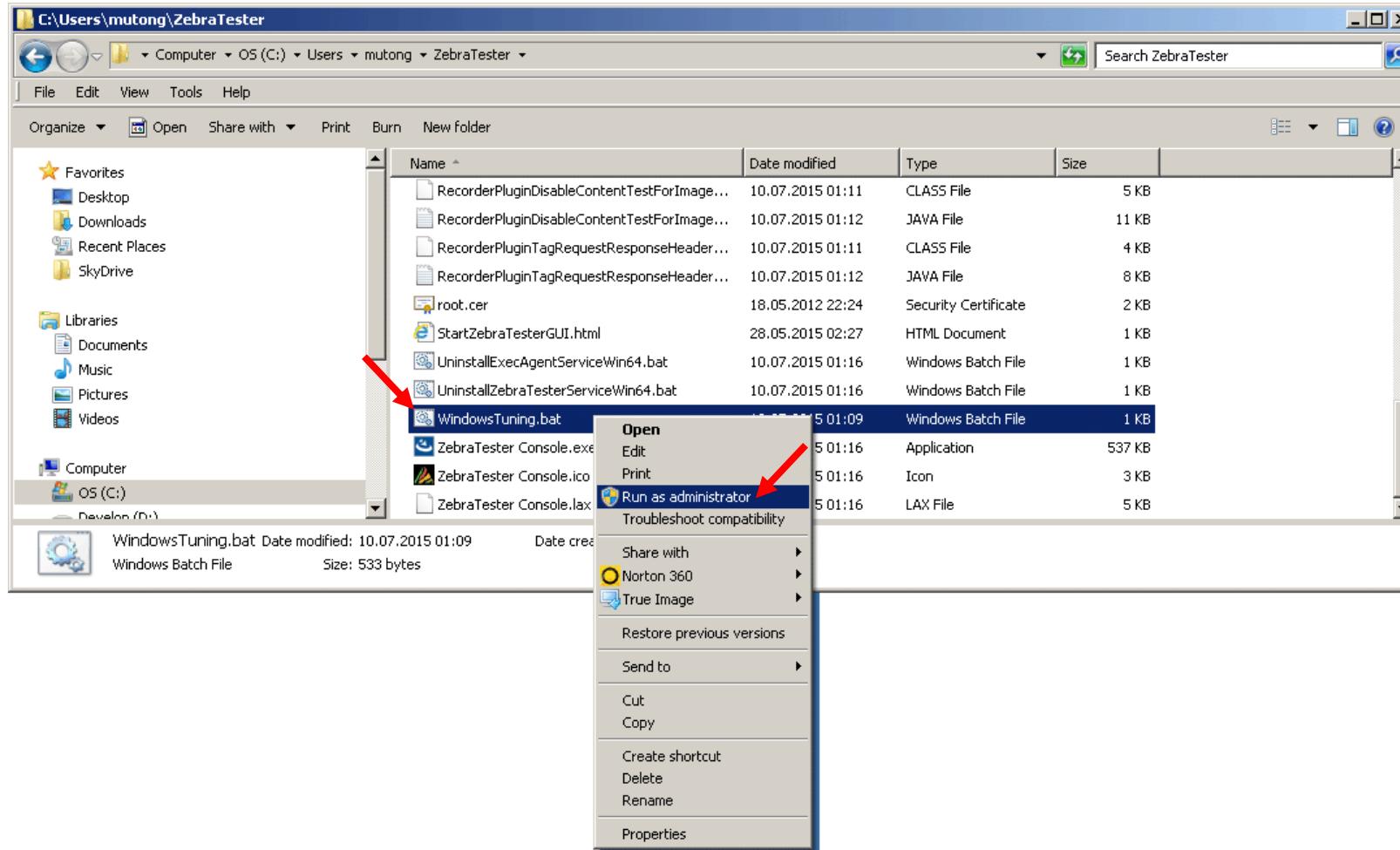
7. Import your CA Root Certificate into Firefox. Enable the checkbox **Trust this CA to identify websites**:

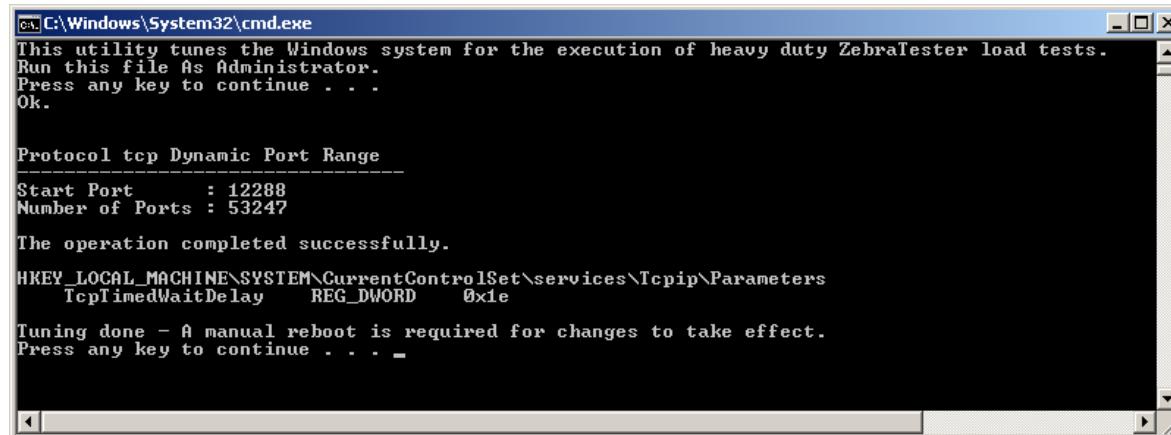


1.3.2 Windows System Tuning

To perform heavy duty load tests from a Windows system you have to tune Windows. Proceed as follows:

1. Open an Explorer Window and navigate to the **ZebraTester installation directory** (typically at C:\Users\<your-name>\ZebraTester).
2. Run the script **WindowsTuning.bat** as **Administrator**:





The screenshot shows a command-line interface (cmd.exe) window titled 'C:\Windows\System32\cmd.exe'. The window contains the following text:

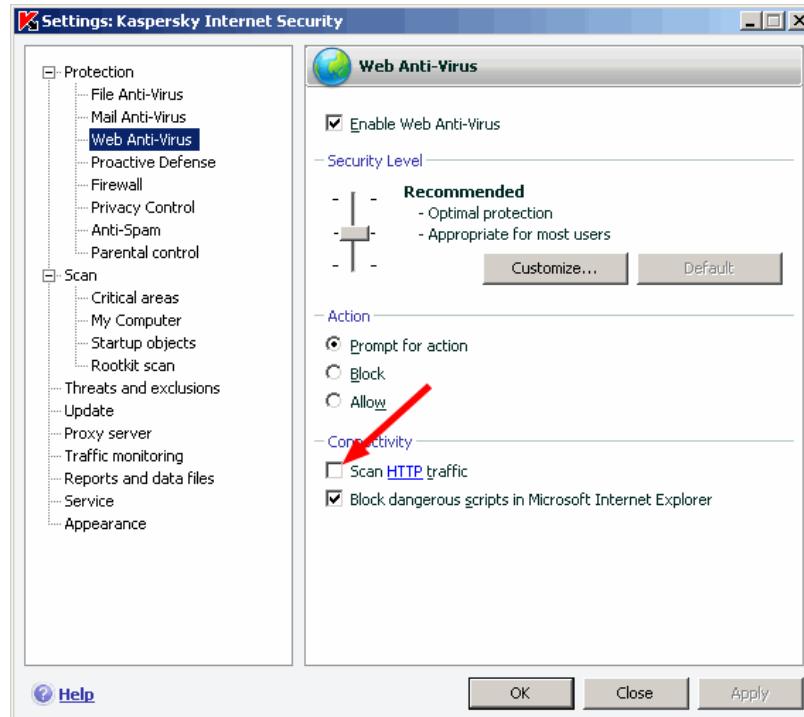
```
This utility tunes the Windows system for the execution of heavy duty ZebraTester load tests.  
Run this file As Administrator.  
Press any key to continue . . .  
Ok.  
  
Protocol tcp Dynamic Port Range  
-----  
Start Port : 12288  
Number of Ports : 53247  
The operation completed successfully.  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters  
    TcpTimedWaitDelay    REG_DWORD    0x1e  
Tuning done - A manual reboot is required for changes to take effect.  
Press any key to continue . . . -
```

Reboot the machine for changes to take effect.

1.3.2.1 Disabling HTTP/S Anti-Virus Network-Scanning

Almost all anti-virus products support to scan the HTTP/S network traffic but they are often not able to handle the load released by a load test – and they delay also the measured response times. Therefore we recommend that you **disable scanning of HTTP/S network connections for viruses. Please note that you should not disable completely your virus scanner. Especially scanning the Disk I/O for viruses should be still enabled.**

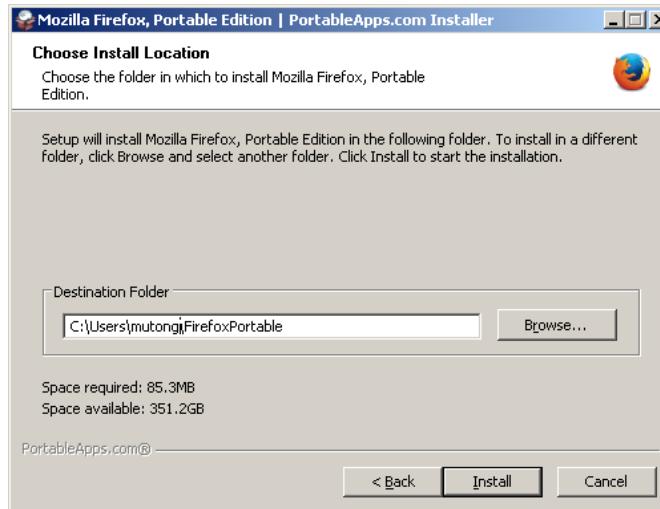
The following picture shows as an example how to disable HTTP/S anti-virus scanning in Kaspersky:



We recommend that you re-enable HTTP/S anti-virus scanning after the execution of your load tests has been completed.

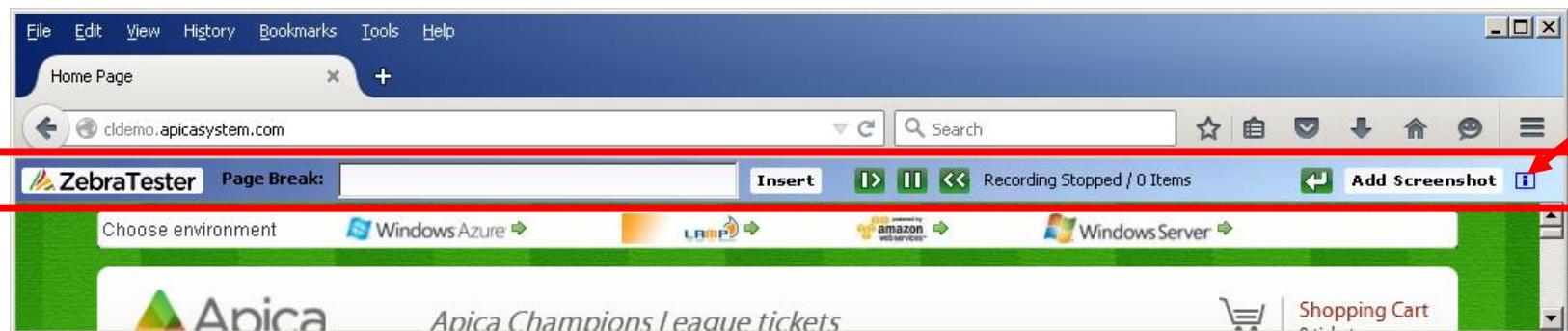
1.3.3 Further Hints for using ZebraTester on Windows - Firefox Portable and Firefox Recording Extension

Accessing the ZebraTester GUI and recording of Web surfing sessions is fully supported by using the Microsoft Internet Explorer (see chapter 3). However, to record Web surfing sessions in a more convenient way, and to avoid any reconfiguration of your standard Web browser, we recommend that you download the **Firefox Portable** Web Browser from http://portableapps.com/apps/internet/firefox_portable and install it inside your C:\Users\<your-name>\FirefoxPortable directory:



After that you should download the **Firefox Recording Extension** from http://www.zebratester.ch/download/zebratester_recording_extension-3.4003-fx.zip. (unzip the content to a local folder after download)

Then start the **Firefox Portable** Web Browser and install the **Firefox Recording Extension (ZebraTester Toolbar)** by using the Firefox Menu Bar → File → Open File ... **zebratester_recording_extension-3.4003-fx.xpi**



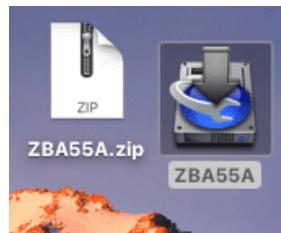
Note: Using the **Firefox Recording Extension** requires that the **ZebraTester Console** is started.

Important Note:

During the normal operation of the Firefox Web browser – when no Web browser sessions should be recorded – it is strongly recommended that **all activity of this extension be disabled**. This can easily be done by **disabling the “ZebraTester Toolbar”** in the Web browser menu “View” ➔ “Toolbars”.

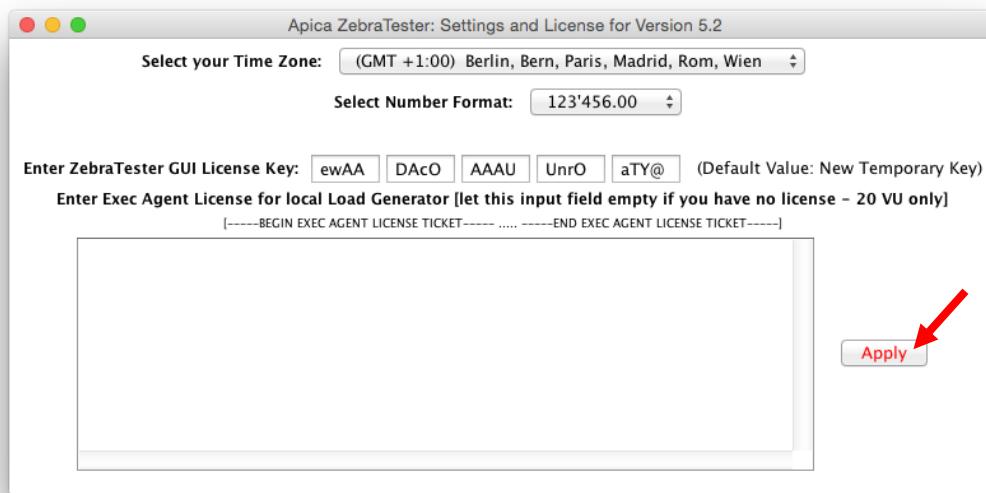


1.4 Installation on Mac OS X / macOS



Expand the archive **ZBA55<minor version>.zip** with a mouse click and then start the installation by clicking on **ZBA55<minor version>**. Follow the installation instructions. We recommend to install ZebraTester into the proposed folder **/Applications/ZebraTester**. Alternatively, you can install ZebraTester in any other location like your home folder **/Users/<your account name>/ZebraTester**.

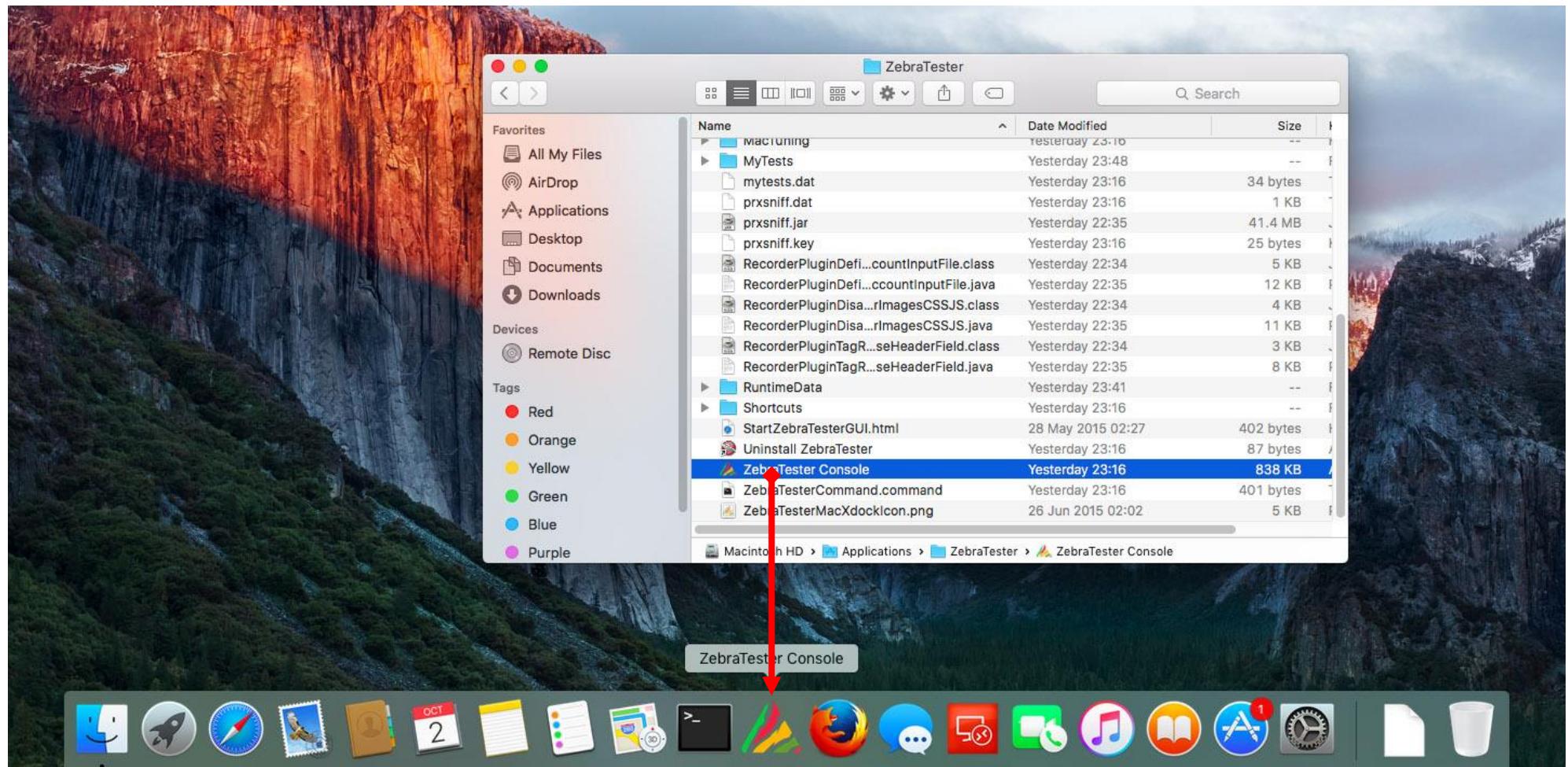
During the installation a popup window is shown which generates a new default license, or shows your existing license if ZebraTester was already installed earlier at the same location. **Note that you must click on the Apply button** in order that the new license is stored on disk.



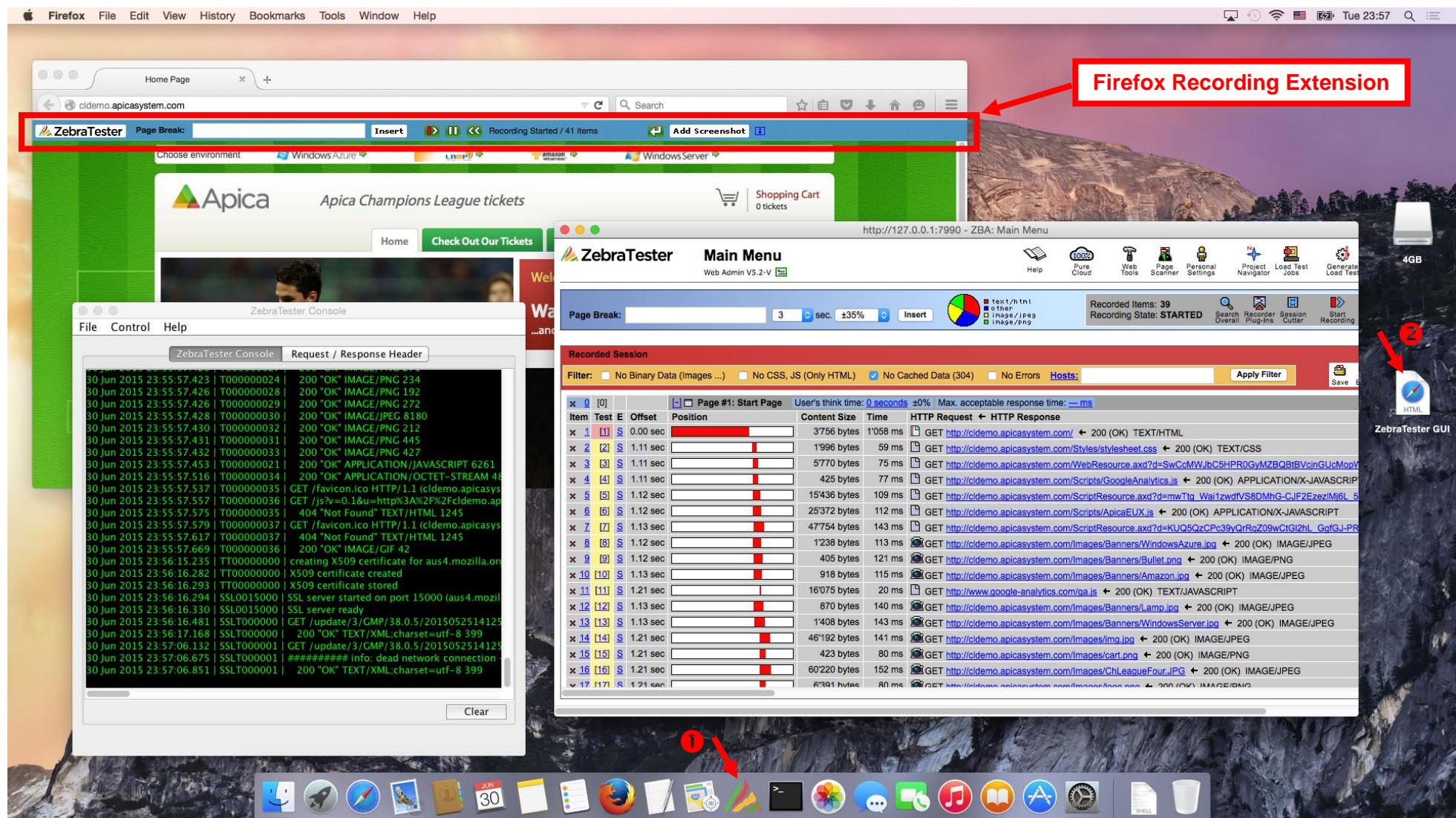
After installation, a new hyperlink icon is placed on your desktop for accessing the (local) ZebraTester Web GUI. If you wish, you can delete this desktop icon.

Open now a Finder window and navigate to the installation directory **/Applications/ZebraTester**

We recommend that you drag the "ZebraTester Console" shortcut to the Dock.

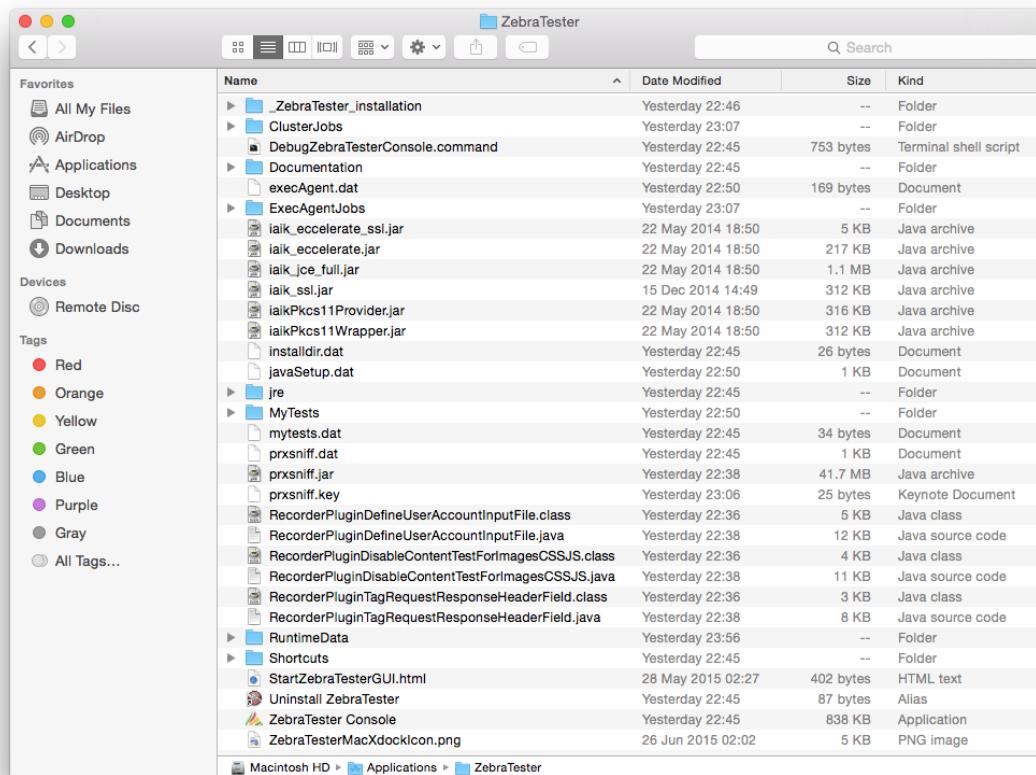


Start ZebraTester by clicking first on the **ZebraTester Console** icon, and then by clicking on the **ZebraTester GUI** icon (Safari). Alternatively you can also access the GUI by starting the **Firefox Web Browser** and entering <http://127.0.0.1:7990> into Firefox. The **Firefox Recording Extension** is also supported on Mac OS X systems (see chapter 3) which allows the Recording of Web Surfing Sessions in a convenient way.



Further Hints:

- The ZebraTester documentation is located inside the subdirectory **Documentation**.
- ZebraTester can be uninstalled by clicking on the **Uninstall ZebraTester** icon. Note that your recorded Web sessions and your load tests are not deleted by the uninstall procedure.
- For security reasons we strongly recommend that you **generate your own CA root certificate** for ZebraTester and import this root certificate into the OS (for Safari) and/or into Firefox (see next subchapter).
- We recommend that you **tune your Mac OS X system** (see second subchapter).
- We recommend that you **add the Firefox Recording Extension** to Firefox (see chapter 3).

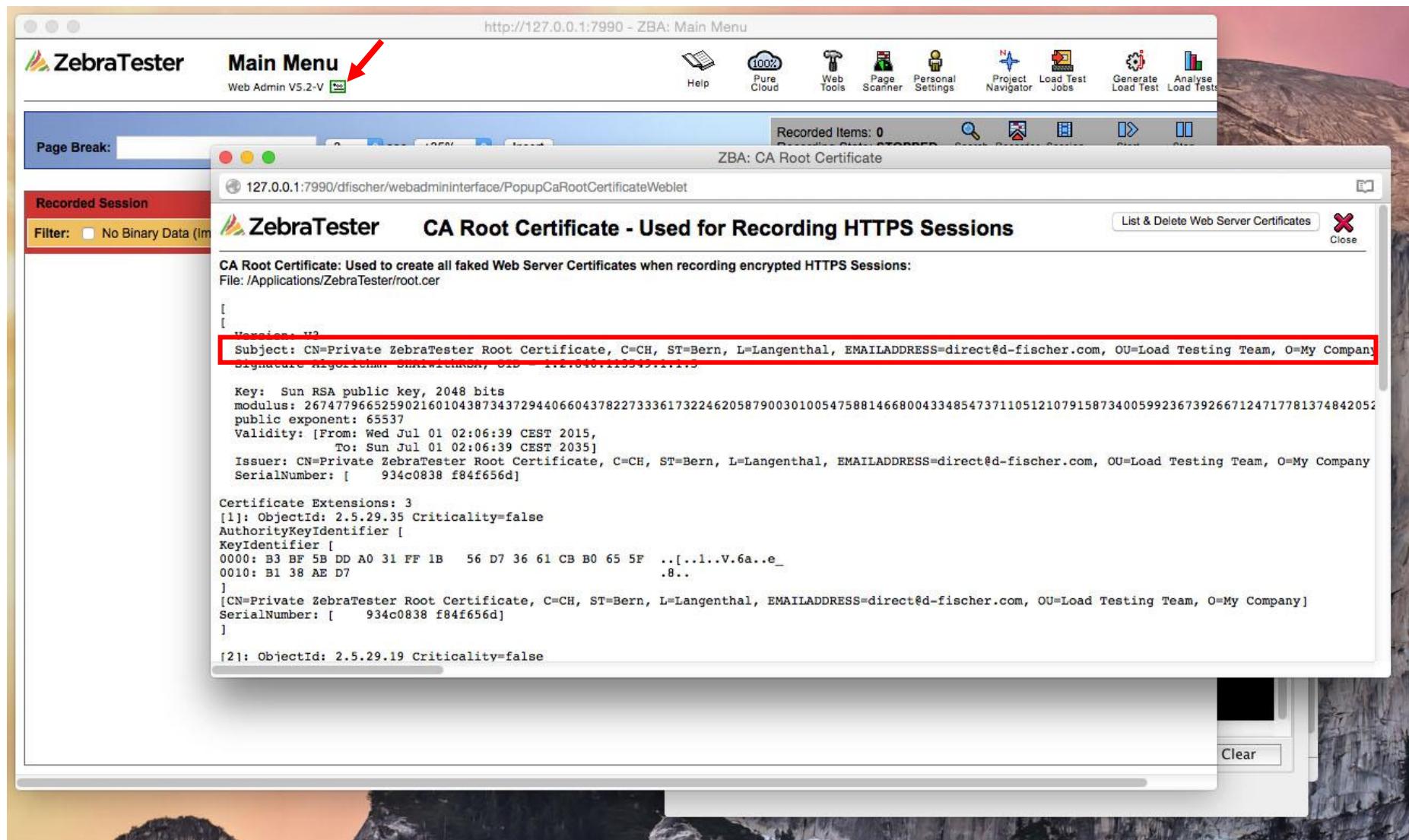


1.4.1 Generating an own, private CA Root Certificate on Mac OS X / macOS

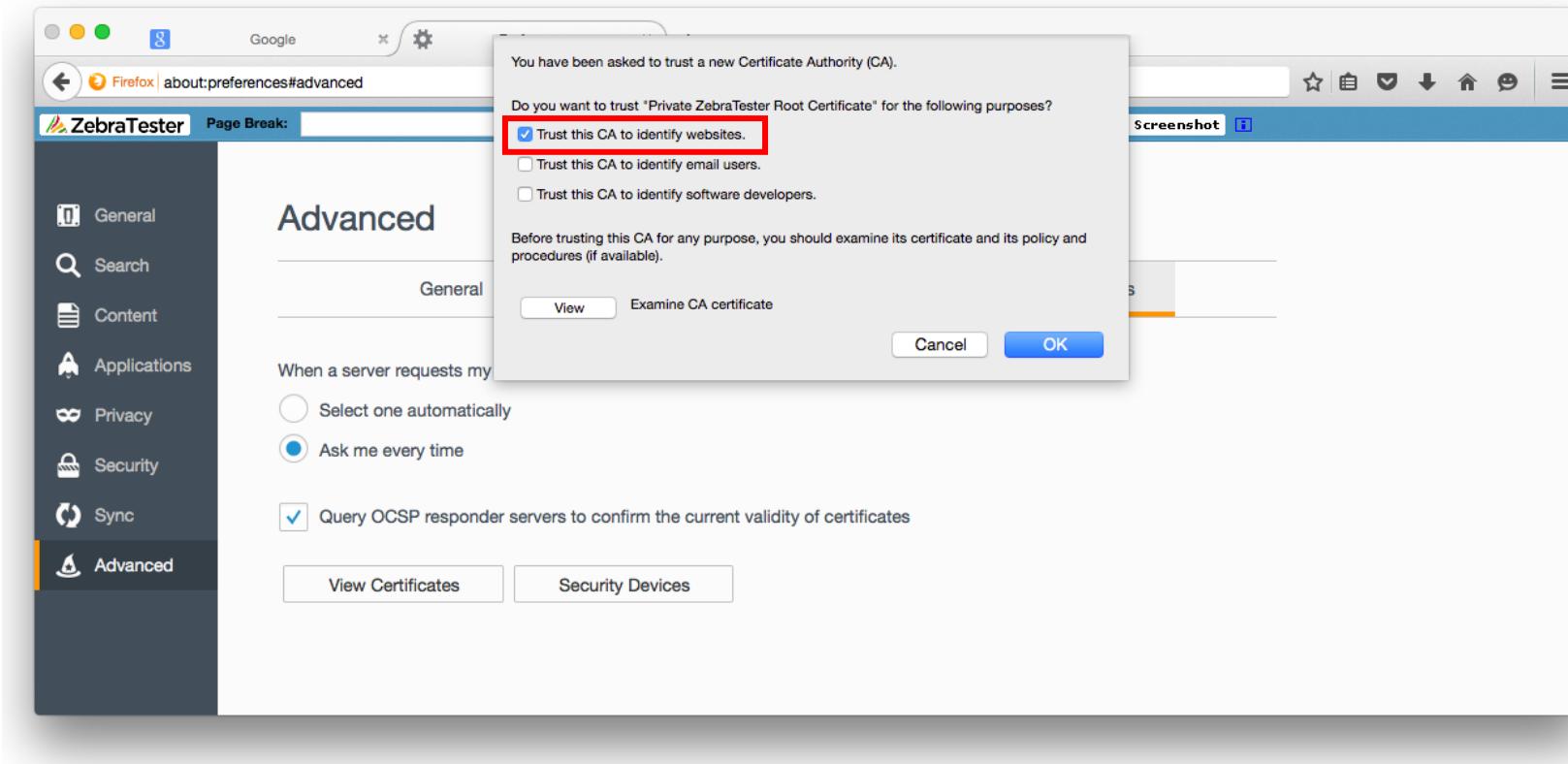
1. Open a Finder window and navigate to the **installation subdirectory /RuntimeData** (typically at /Applications/ZebraTester/RuntimeData)
2. Click on **CreateOwnCARootCertificate.command**
3. Enter any obvious input for your private CA Root Certificate:

```
This utility generates an own, private CA root certificate for ZebraTester. Enter <return> to continue
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'privkey.pem'
-----
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Organization Name (company) [My Company]:My Company
Organizational Unit Name (department, division) []:Load Testing Team
Email Address []:direct@d-fischer.com
Locality Name (city, district) [My Town]:Langenthal
State or Province Name (full name) [State or Providence]:Bern
Country Name (2 letter code) [US]:CH
Common Name (hostname, IP, or CA name) []:ZebraTester Root Certificate (Karl Smith)
Your own CA root certificate was generated
Restart ZebraTester and import /Applications/ZebraTester/RuntimeData/root.cer into the OS and/or into Firefox
```

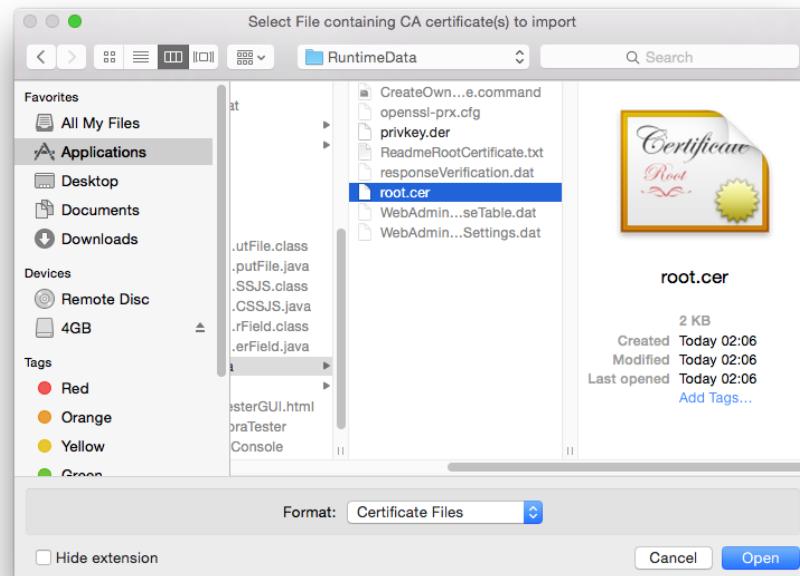
4. Restart the ZebraTester Console and verify your CA Root Certificate using the Web Admin GUI:



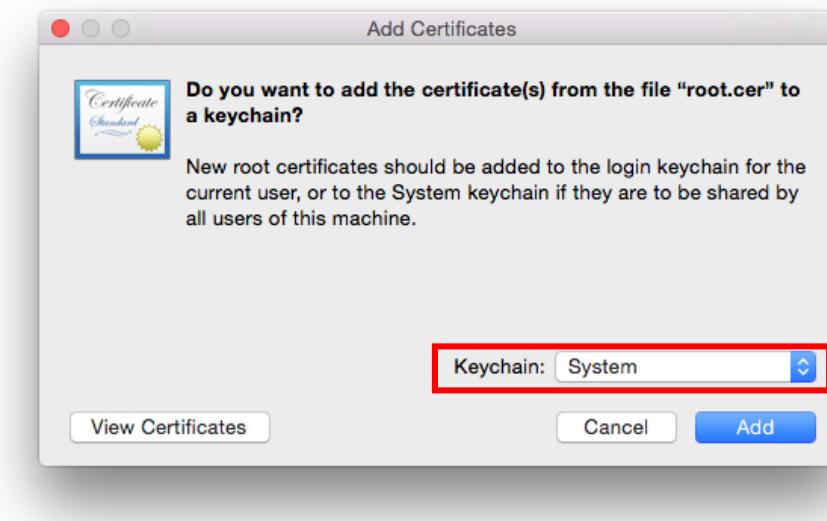
5. Import your CA Root Certificate into Firefox. Select the file **root.cer** in the ZebraTester installation subdirectory **/RuntimeData**. Enable the checkbox "Trust this CA to identify websites":

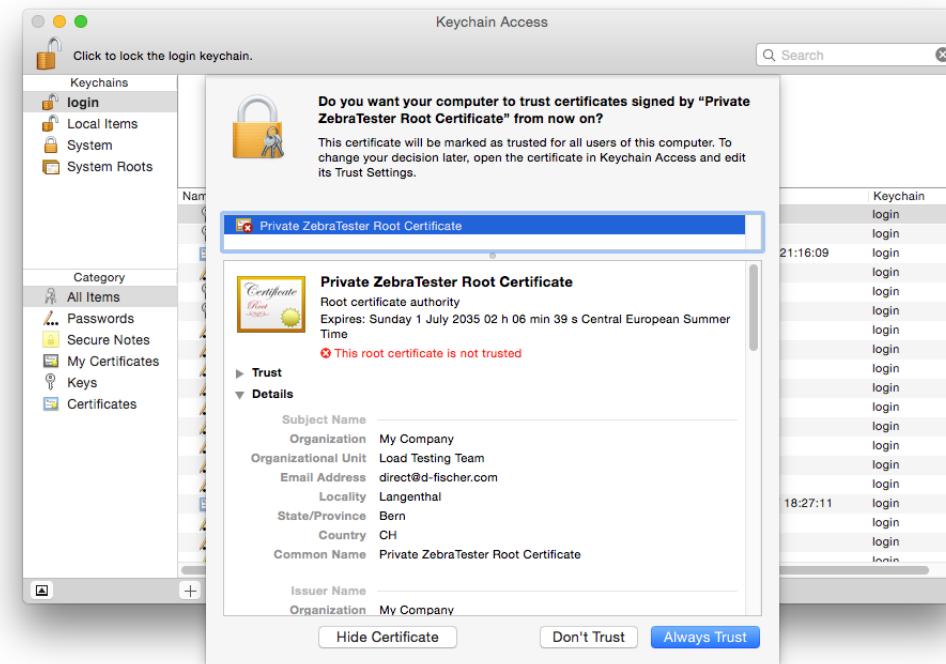


6. Import your CA Root Certificate into Mac OS X (for Safari)



Select the "System" keychain:





Hint: See Appendix A at the end of this document to learn how to Import your CA Root Certificate into an Apple iOS device (iPhone and iPad).

1.4.2 Mac OS X / macOS System Tuning

The OS-settings for the maximum number of network connections per process is restricted by default to a value of 256 on almost all Mac OS X versions. You can verify this value by entering the command "**ulimit -n**" from a terminal. This default value is too small to execute even small load tests from Mac OS X systems and it is also too small to monitor remotely executed cluster jobs executed on any other machines.

We recommend that you tune your Mac OS X / macOS system.

To review the default (non-tuned) settings:

1. Enter "**ulimit -n**". Typically you will see:
256
2. Enter "**launchctl limit**". Typically you will see:
maxproc 709 1064
maxfiles 256 unlimited

Tuning instructions:

1. Open a Finder window and navigate to the **installation subdirectory /MacTuning** (typically at /Applications/ZebraTester/MacTuning)
2. Click on **DoMacTuning.command**
3. A terminal window appears. Enter first <return> to continue and then enter the superuser password (sudo root password)

```
Last login: Wed Jul 1 23:11:17 on console
Davids-Air:~ fischer$ /Applications/ZebraTester/MacTuning/DoMacTuning.command ; exit;
This utility tunes the MAC OS X system. Enter <return> to continue

WARNING: Improper use of the sudo command could lead to data loss
or the deletion of important system files. Please double-check your
typing when using sudo. Type "man sudo" for more information.

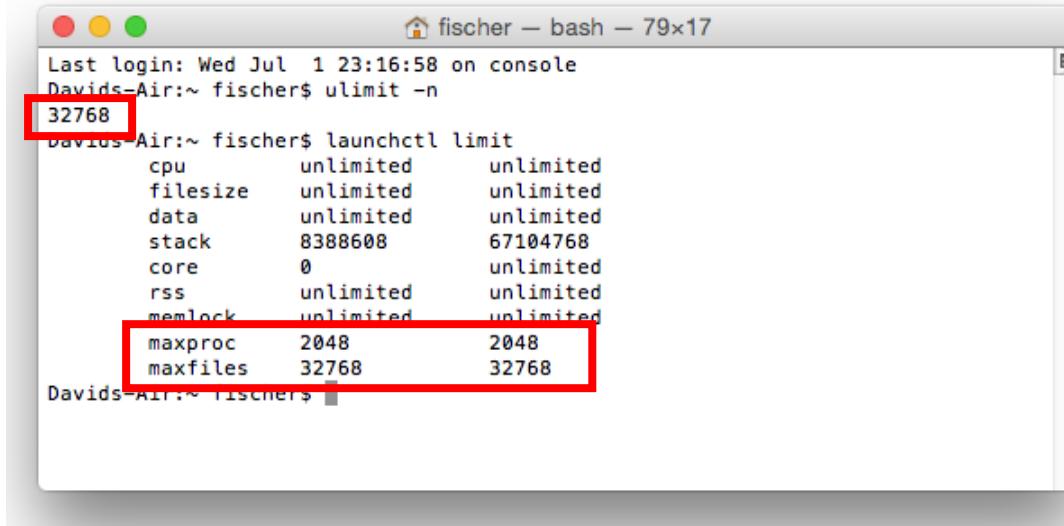
To proceed, enter your password, or type Ctrl-C to abort.

Password:
kern.maxfiles: 12288 -> 32768
kern.maxfilesperproc: 10240 -> 32768
kern.maxproc: 1064 -> 2048
kern.maxprocperuid: 709 -> 2048
ZebraTester.tuning.maxfiles.plist -> /Library/LaunchDaemons/ZebraTester.tuning.maxfiles.plist
ZebraTester.tuning.maxproc.plist -> /Library/LaunchDaemons/ZebraTester.tuning.maxproc.plist

Tuning done.
You must reboot the machine to take effect.
logout

[Process completed]
```

4. Restart the Mac OS X / macOS system (reboot).
5. Verify the new settings after the restart. Open a terminal window and enter "**ulimit -n**" and "**launchctl limit**"



```
Last login: Wed Jul  1 23:16:58 on console
Davids-Air:~ fischer$ ulimit -n
32768
Davids-Air:~ fischer$ launchctl limit
cpu      unlimited      unlimited
filesize unlimited      unlimited
data     unlimited      unlimited
stack    8388608      67104768
core     0            unlimited
rss      unlimited      unlimited
memlock  unlimited      unlimited
maxproc  2048         2048
maxfiles 32768        32768
Davids-Air:~ fischer$
```

1.4.3 Using a Public JDK on Mac OS X / macOS

We recommend to use always the (private) Java installation which is delivered by the ZebraTester installation kit.
→ In such a case you can skip this chapter.

In case if you use another public JDK for ZebraTester you have to **add manually** a new Java security provider called "**iaik.security.provider.IAIK**" which is required for ZebraTester. If you miss this step ZebraTester will not work correctly.

1. Locate the file named "**java.security**" on your computer by entering

```
sudo find / -name "java.security" -print
```

from a terminal. Typically this file is found in the following directory:

/System/Library/Java/JavaVirtualMachines/1.6.0.jdk/Contents/Home/lib/security or
/Library/Java/JavaVirtualMachines/jdk1.7.0_09.jdk/Contents/Home/jre/lib/security

2. Edit this file by entering the command

```
sudo vi java.security
```

and add the IAIK security provider at the last position. Example:

```
#  
# MacOSX added com.apple.crypto.provider.Apple as #3  
security.provider.1=sun.security.pkcs11.SunPKCS11 ${java.home}/lib/security/sunpkcs11-macosx.cfg  
security.provider.2=sun.security.provider.Sun  
security.provider.3=com.apple.crypto.provider.Apple  
security.provider.4=sun.security.rsa.SunRsaSign  
security.provider.5=com.sun.net.ssl.internal.ssl.Provider  
security.provider.6=com.sun.crypto.provider.SunJCE  
security.provider.7=sun.security.jgss.SunProvider  
security.provider.8=com.sun.security.sasl.Provider  
security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI  
security.provider.10=sun.security.smartcardio.SunPCSC  
security.provider.11=iaik.security.provider.IAIK
```

1.5 Installation on Linux

The standard Linux distributions contain normally no preinstalled JDK (Java Development Kit from Oracle). Therefore you have first to install the original JDK 1.7 from Oracle.

Note: Running ZebraTester with JDK 1.8 from Oracle is also supported (instead of JDK 1.7) but in this case you cannot use the Apica Load Test Portal and you cannot use our predefined Amazon EC2 load generators.

In case you have installed the JDK from Oracle by downloading the “**Java SE Development Kit**” *.tar.gz file please ensure that the PATH to the java JDK is available for all OS processes. Therefore you should add the PATH to the binaries of the “Java SE Development Kit” to the following files (require root privileges):

- /etc/environment
- /etc/profile

Example for /etc/environment:

```
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/java/jdk1.7.0_80/bin"
```

Example for /etc/profile:

```
if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi

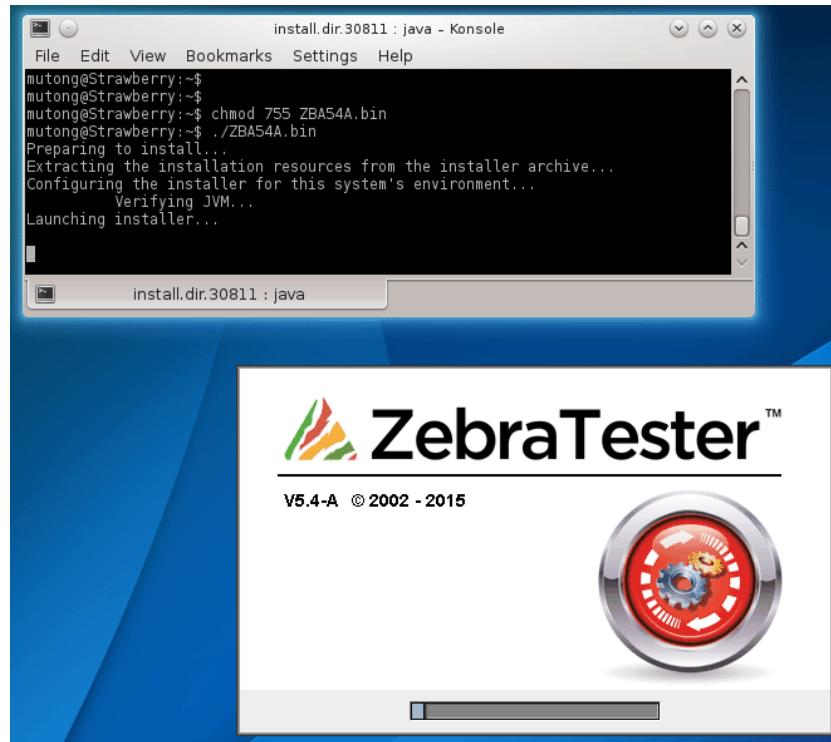
PATH=$PATH:/java/jdk1.7.0_80/bin
export PATH
```

Note: Depending on your Linux distribution it might be also necessary to set the environment variable **JAVA_HOME** which should point to the “Java SE Development Kit” main folder. Example:

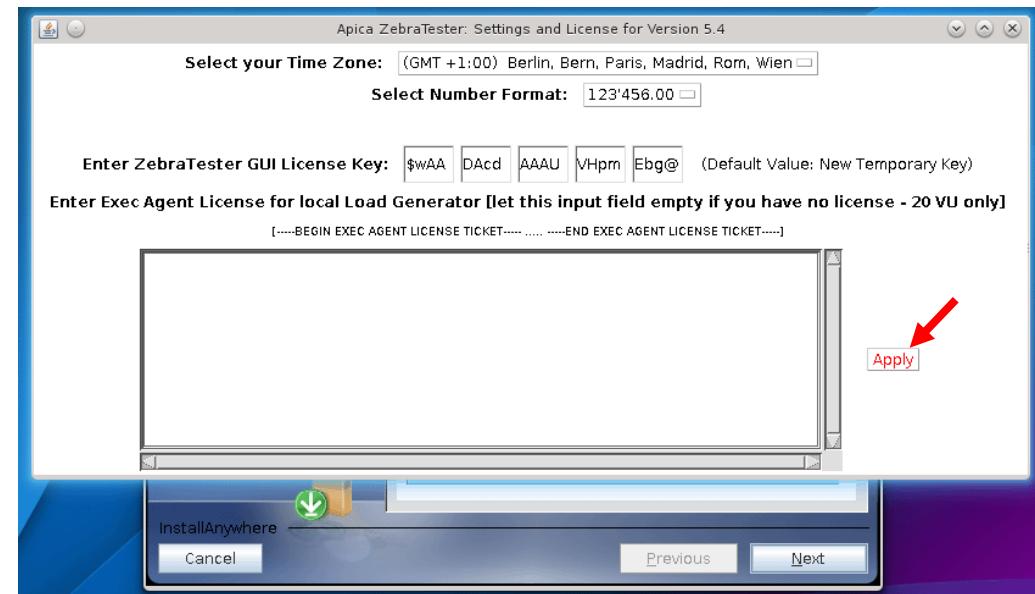
```
JAVA_HOME=/java/jdk1.7.0_80
export JAVA_HOME
```

Once Java is installed proceed as follows:

1. Download **ZBA55<minor version>.bin** and save it in your home folder.
2. Open a terminal and change the file permission of ZBA54<minor version>.bin so that it can be executed:
`chmod 755 ZBA55<minor version>.bin`
3. After that start the installation by entering:
`./ZBA55<minor version>.bin`
4. Note: ZBA55<minor version>.bin can be deleted after installation.

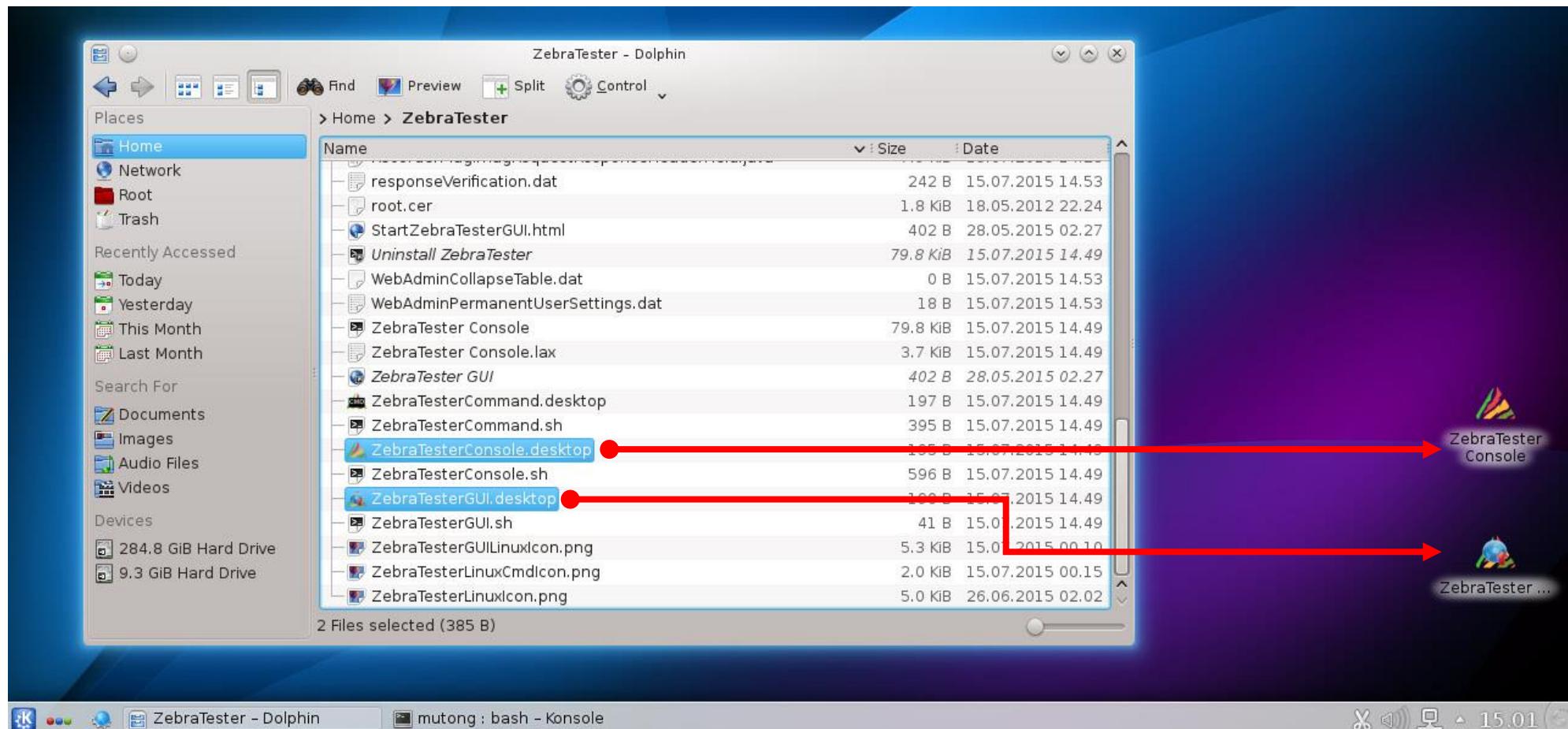


During the installation a popup window is shown which generates a new default license, or shows your existing license if ZebraTester was already installed earlier at the same location. **Note that you must click on the Apply button** in order that the new license is stored on disk.

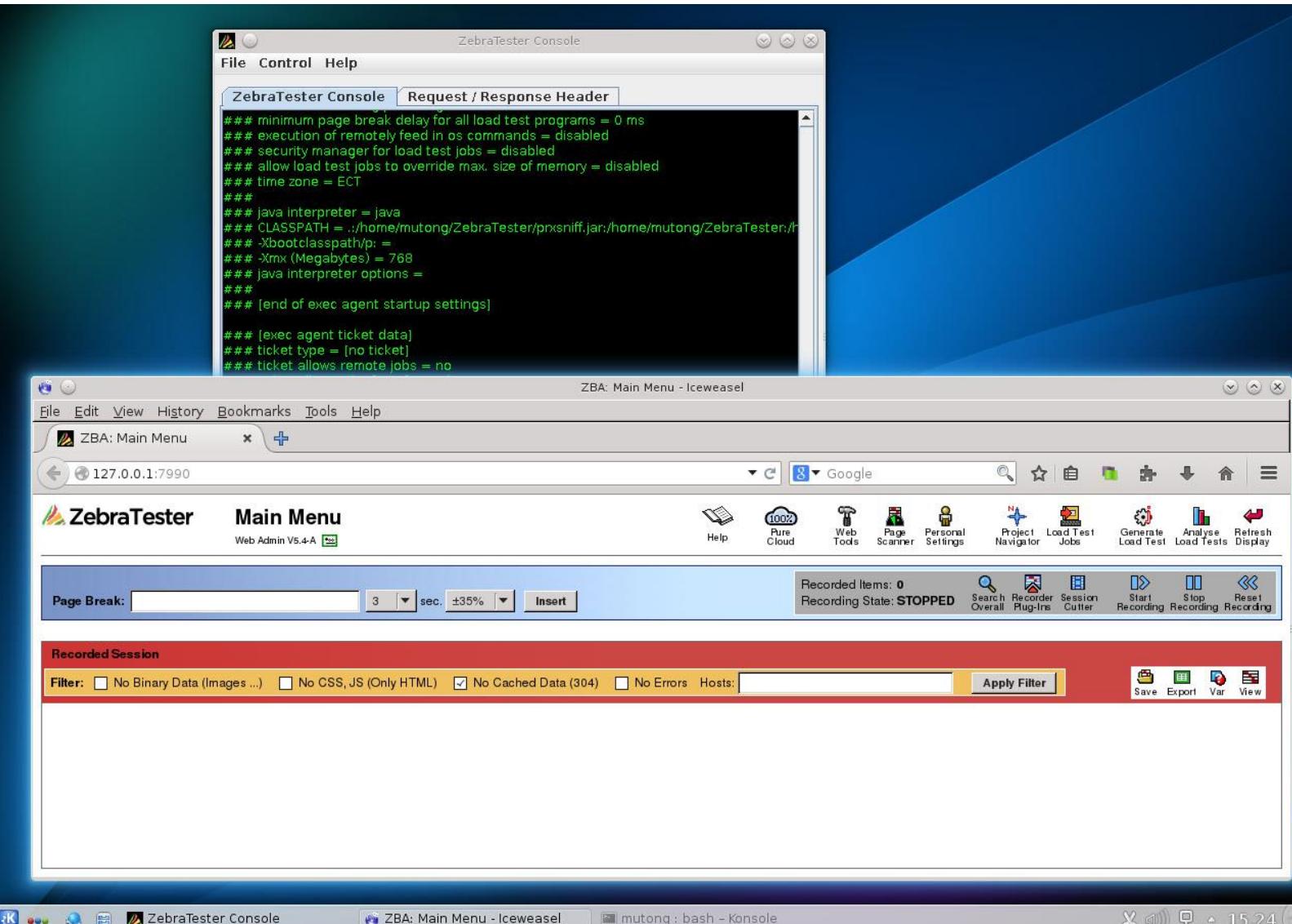


Open now a File Manager window and navigate to the ZebraTester installation directory.

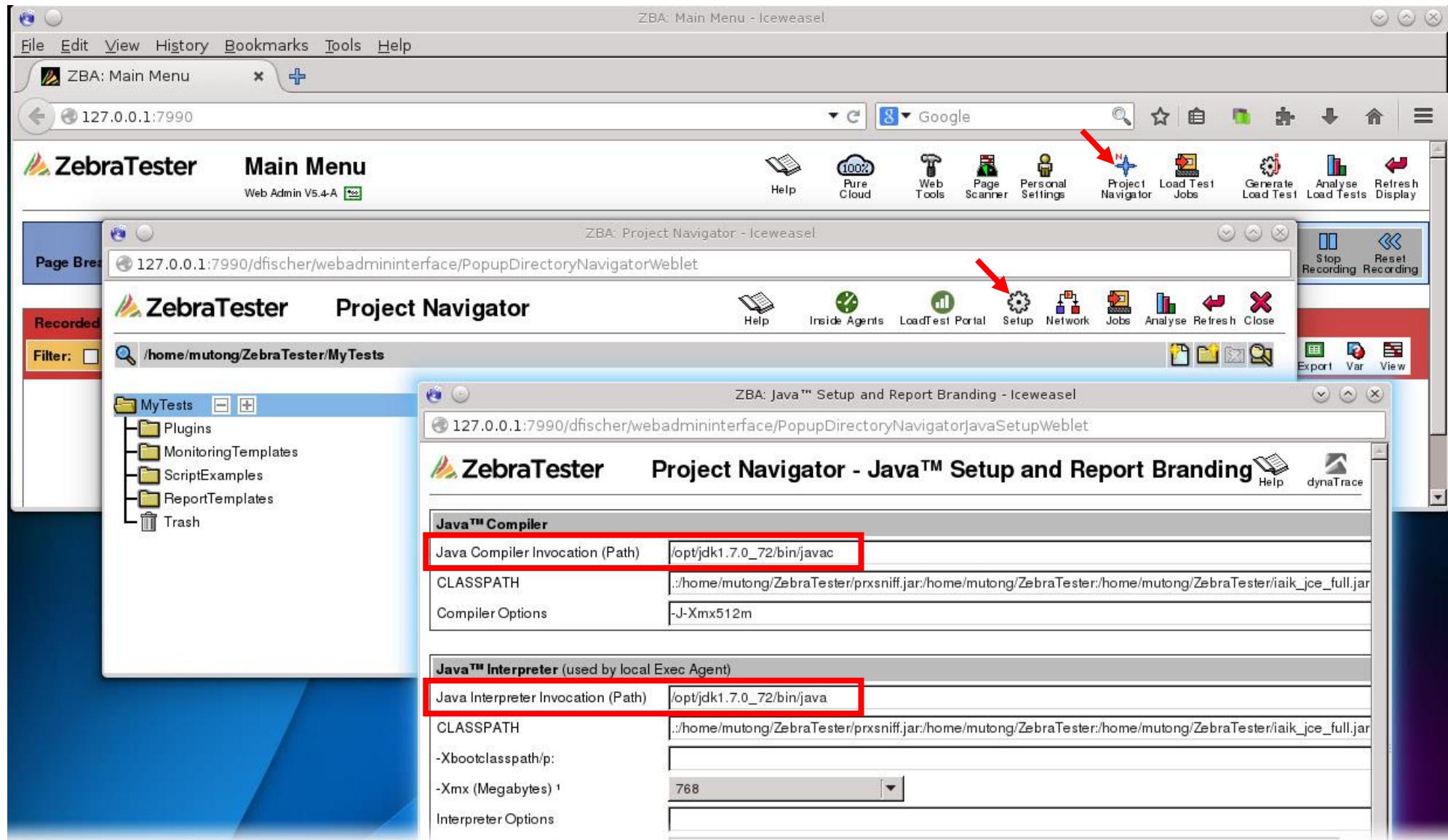
We recommend that you drag the files "ZebraTesterConsole.desktop" and "ZebraTesterGUI.desktop" to the desktop.



Start ZebraTester by clicking first on the **ZebraTester Console** icon, and then by clicking on the **ZebraTester GUI** icon. Alternatively you can also access the GUI by starting any **Web Browser** and entering <http://127.0.0.1:7990> (Firefox or Iceweasel recommended). The **Firefox Recording Extension** is also supported on Linux systems which allows the Recording of Web Surfing Sessions in a convenient way.



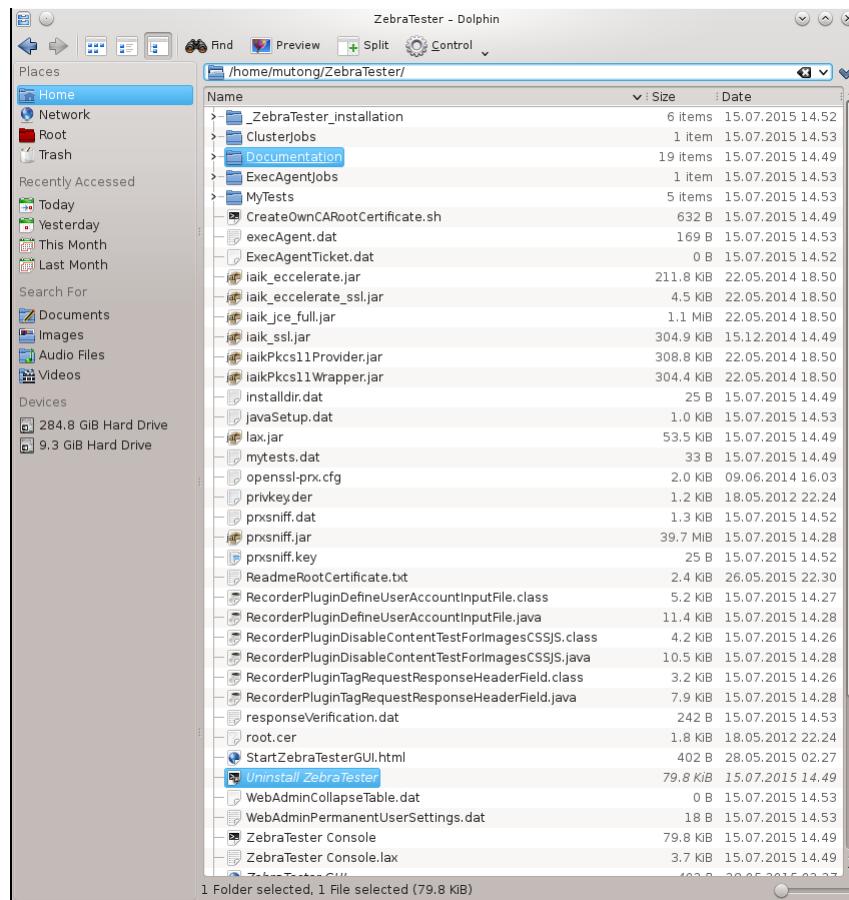
If you have **multiple versions of Java** installed then you should ensure that ZebraTester is using the right Java 1.7 version (Oracle 7 JDK). Click in the ZebraTester GUI on **Project Navigator → Settings** and verify and/or modify the path to the **Java 7 compiler** and to the **Java 7 interpreter**:



Further Hints:

- The ZebraTester documentation is located inside the subdirectory **Documentation**.

- ZebraTester can be uninstalled by clicking on **Uninstall ZebraTester**. Note that your recorded Web sessions and your load tests are not deleted by the uninstall procedure.
- For security reasons we strongly recommend that you **generate your own CA Root Certificate** for ZebraTester and import this root certificate into the OS and/or into Firefox (see next subchapter).
- We recommend that you **tune your Linux system** (see second subchapter).
- We recommend that you **add the Firefox Recording Extension** to Firefox (see chapter 3).



1.5.1 Generating an own, private CA Root Certificate on Linux

1. Open a File Manager window and navigate to the ZebraTester installation directory
2. Click on **ZebraTesterCommand.desktop** → A terminal windows appears
3. Enter the following command into the terminal window:
`./CreateOwnCARootCertificate.sh`
4. Enter any obvious input for your private CA Root Certificate:

```
This utility generates an own, private CA root certificate for ZebraTester. Enter <return> to
continue./CreateOwnCARootCertificate.sh: 2: read: arg count
```

```
Generating a 2048 bit RSA private key
```

```
.....+++
```

```
.....+++
```

```
writing new private key to 'privkey.pem'
```

```
----
```

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
```

```
----
```

```
Organization Name (company) [My Company]:My Company
```

```
Organizational Unit Name (department, division) []:Load Testing Team
```

```
Email Address []:direct@d-fischer.com
```

```
Locality Name (city, district) [My Town]:Langenthal
```

```
State or Province Name (full name) [State or Providence]:Bern
```

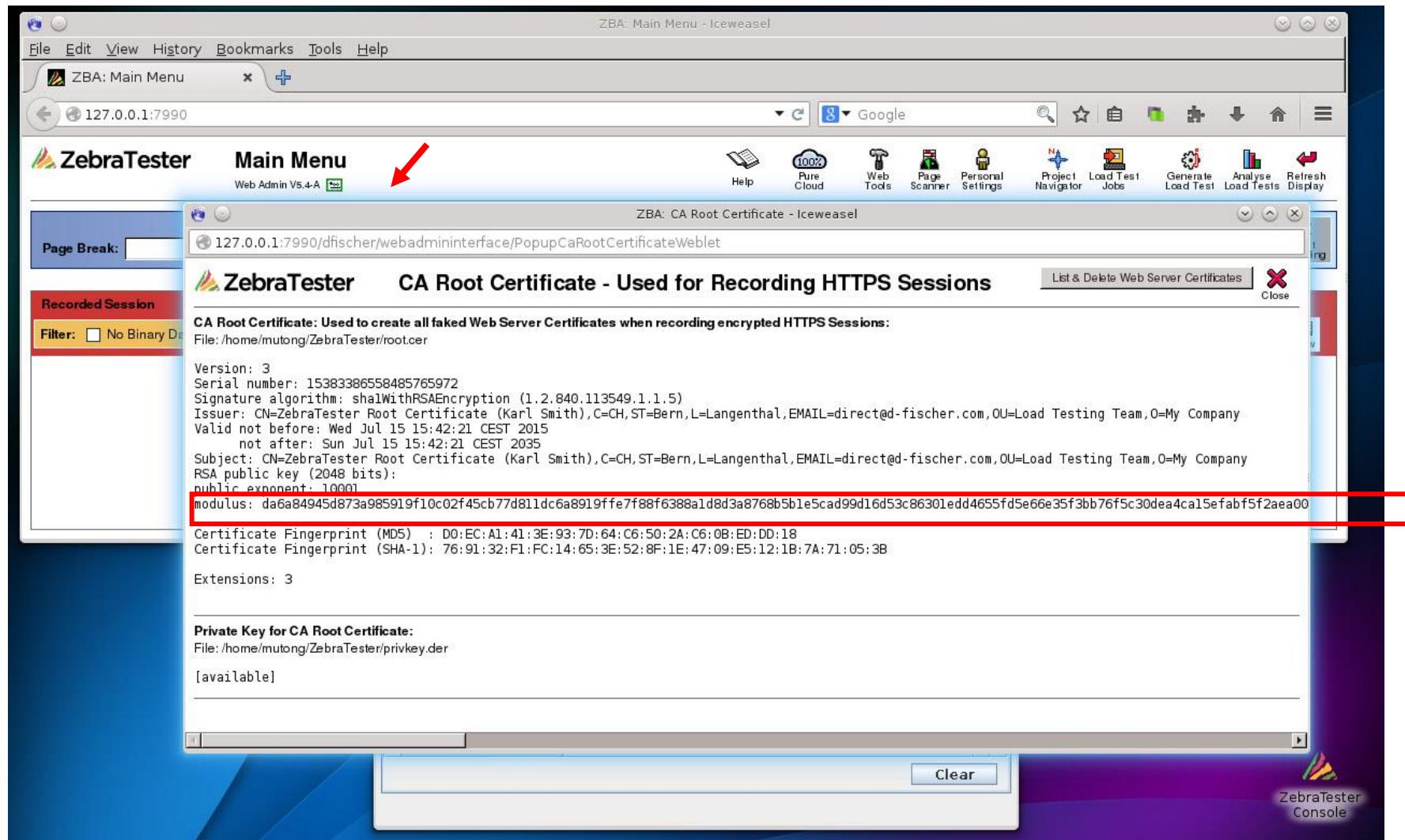
```
Country Name (2 letter code) [US]:CH
```

```
Common Name (hostname, IP, or CA name) []:ZebraTester Root Certificate (Karl Smith)
```

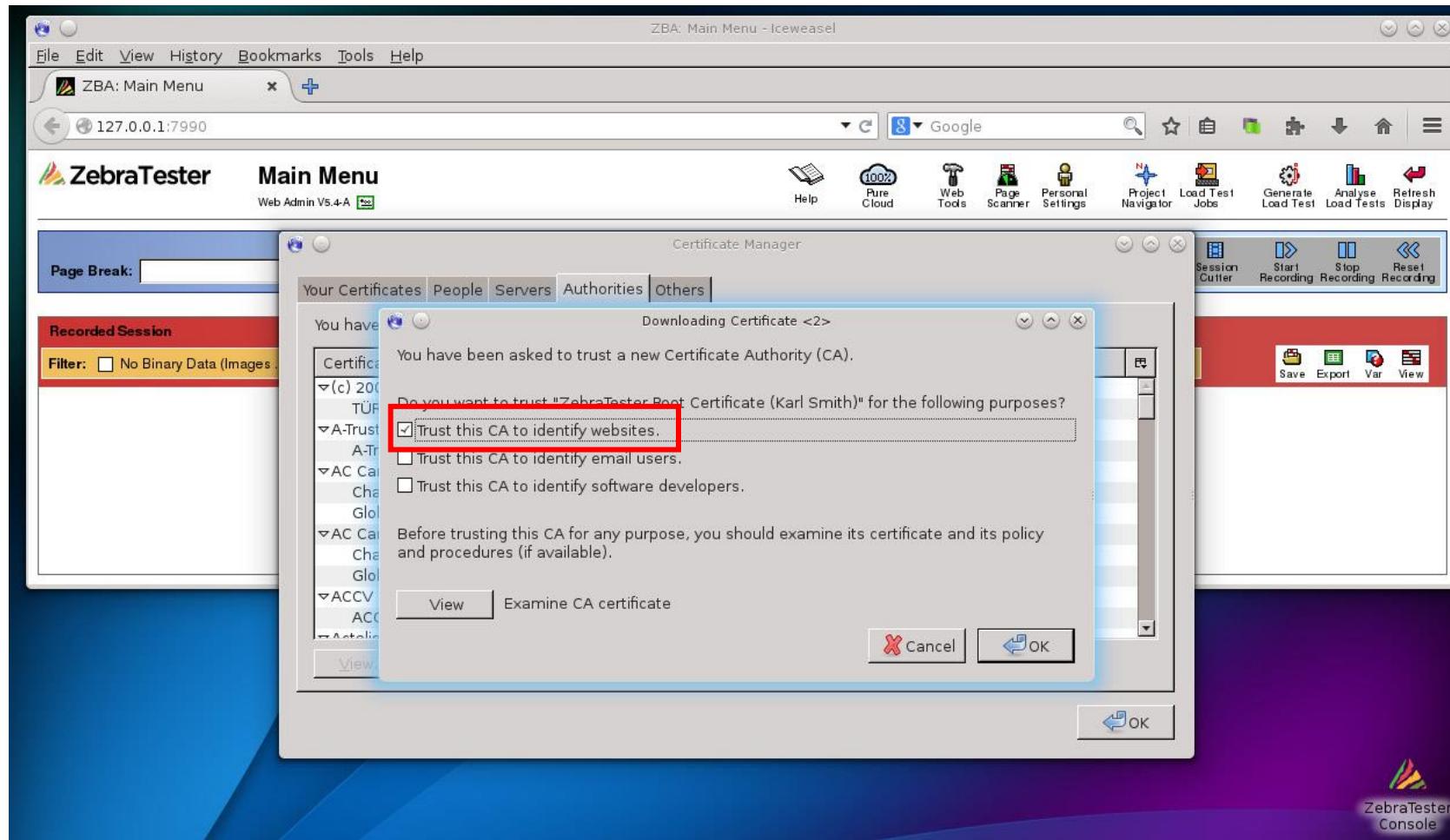
```
Your own CA root certificate was generated
```

```
Restart ZebraTester and import /home/mutong/ZebraTester/root.cer into the OS and/or into Firefox or into Iceweasel
```

5. Restart the ZebraTester Console and verify your CA Root Certificate using the Web Admin GUI:



6. Import your CA Root Certificate into Firefox. Select the file **root.cer** in the ZebraTester installation directory. Enable the checkbox "Trust this CA to identify websites":



1.5.2 Linux Tuning

We recommend that you tune the Linux system. Open a terminal and become root. Then add the following two lines to the file **/etc/sysctl.conf**

```
net.ipv4.ip_local_port_range = 1024 65535  
net.ipv4.tcp_fin_timeout = 30
```

Note: Do **not** set the parameters net.ipv4.tcp_tw_recycle and/or net.ipv4.tcp_tw_reuse to a value of 1. These tuning options are improper for load generators.

Enter also from a terminal the following command:

```
ulimit -n
```

You should see a value greater or equal than 32768 (65536 recommended). If this value is too low you have also to tune the Linux system.

Almost all of the Linux systems do not have enough entropy to generate a large amount of random numbers in a short time. But such random numbers are needed to execute load tests with encrypted network connections (HTTPS). Therefore we strongly recommend to increase the entropy by installing the **haveged daemon** on all Linux systems. See <http://www.issihosts.com/haveged/>

Note that a load test may block/freeze for several minutes if you don't install the haveged daemon.

1.6 Manual Installation on all Unix-like Systems (Linux, Solaris, BSD, Mac OS X ...)

If no installation kit is available for your OS, or if you don't want to use an installation kit, you can perform a manual installation of ZebraTester. Note that a Java 1.7 SDK (Java compiler and interpreter) must already be pre-installed.

1. Manually create the installation directory **/usr/local/ZebraTester** (you may choose also any other installation directory)
2. Copy the files **prxsniff.jar**, **iaik_jce_full.jar**, **iaik_ssl.jar**, **iaik_eccelerate.jar**, **iaik_eccelerate_ssl.jar**, **iaikPkcs11Provider.jar**, **iaikPkcs11Wrapper.jar**, **root.cer** and **privkey.der** to this directory (you can copy this files from a Windows or a Mac OS X installation of ZebraTester. These files can be used for all operating systems).
3. Create or copy the files **prxsniff.key** and **ExecAgentTicket.dat** inside the installation directory. You can use **vi** or another text editor. These files must contain (as ASCII text) the ZebraTester GUI license key and the Exec Agent license ticket.
4. Set the Java **CLASSPATH** environment variable to include **the installation directory**, the default directory ("."), and the path to all *.jar files.
Example: `export CLASSPATH=.:prxsniff.jar:iaik_jce_full.jar:iaik_ssl.jar:iaik_eccelerate.jar:iaik_eccelerate_ssl.jar:iaikPkcs11Provider.jar:iaikPkcs11Wrapper.jar`
5. Start ZebraTester with the following command:
`java -Xmx1024m ProxySniffer -WebAdmin -JobController -ExecAgent -encryptJobsOriginBackup -tz CST`
Hint: the **-tz** argument is the time zone. Chapter 6 of the **Application Reference Manual** contains a list of all time zones.
6. Start a Firefox web browser and enter <http://127.0.0.1:7990>. The **Firefox Recording Extension** is supported on all systems.

Special note for Mac OS X server which do not have an X11 display device (no graphic card installed):

Use `java -Djava.awt.headless=true ...` as additional startup argument

Alternatively to the steps 4 and 5 above you can start on ZebraTester in "GUI Console Mode" by using the following commands:

```
cd /usr/local/ZebraTester
export CLASSPATH=.:prxsniff.jar:iaik_jce_full.jar:iaik_ssl.jar:iaik_eccelerate.jar:iaik_eccelerate_ssl.jar
:iaikPkcs11Provider.jar:iaikPkcs11Wrapper.jar
java -Xmx1024m ProxySnifferConsole -encryptJobsOriginBackup -tz CST
```

Hint: the **-tz** argument is the time zone. Chapter 6 of the **Application Reference Manual** contains a list of all time zones. Note: there are also other useful startup options like **-jobdir** or **-dgs**. Please take a look at chapter 3.1 of the Application Reference Manual.

Note for starting a Load Generator (Exec Agent) as an Independent Process (without ZebraTester GUI): Please take a look at chapter 3.3 of the **Application Reference Manual**. Example:

```
nohup java -Xmx1024m ExecAgent -tz ECT 2>&1 > ExecAgent.log &
```

1.6.1 Generating an own, private CA Root Certificate on Unix-Like Systems

The "Proxy Recorder" of ZebraTester use a common CA Root Certificate (file name = root.cer) for all on the fly generated (faked) HTTPS Web server certificates. This common CA Root Certificate is delivered as a part of the ZebraTester installation kit and could be directly imported in any operating system and in any Web Browser product in order to suppress Web Browser warnings about non-trusted Web server certificates. But consider that all other customers are also able to generate faked HTTPS Web server certificates by using the same CA root certificate delivered by the installation kit !!!.
Therefore, if you import the file "root.cer" delivered by the ZebraTester installation kit into your operating system and/or into your Web Browser the Security of your machine will be severely damaged. You would trust to any Web server certificate issued by any other customer of ZebraTester.

To keep your machine secure we strongly recommend that you do not import the default CA root certificate "root.cer" delivered by the ZebraTester installation kit.

Instead of that **we recommend that you create our own (private) CA Root Certificate** by using OpenSSL (OpenSSL is not part of the ZebraTester installation kit). Proceed as follows:

1. `openssl req -newkey rsa:2048 -sha256 -days 7305 -x509 -nodes -out root.cer` (create your new CA root certificate)
2. `openssl pkcs8 -topk8 -nocrypt -in privkey.pem -outform der -out privkey.der` (then convert the private key)
3. `rm privkey.pem` (no longer needed)

After that **replace** in the ZebraTester installation directory the two files **root.cer** and **privkey.der** with your own versions.

Then remove all previously generated "faked" Web server certificates: **Delete** all ***.crt** and ***.privkey** files.

Finally restart ZebraTester.

Now you can import our own (private) CA root certificate into the operating system and into any Web Browser product in order to prevent Web Browser warnings. Your machine is as long secure as you don't share your own, private CA root key (file `privkey.der`) with anybody else.

► **See also:**

[Generating an own, private CA Root Certificate on Windows](#)

[Generating an own, private CA Root Certificate on Mac OS X](#)

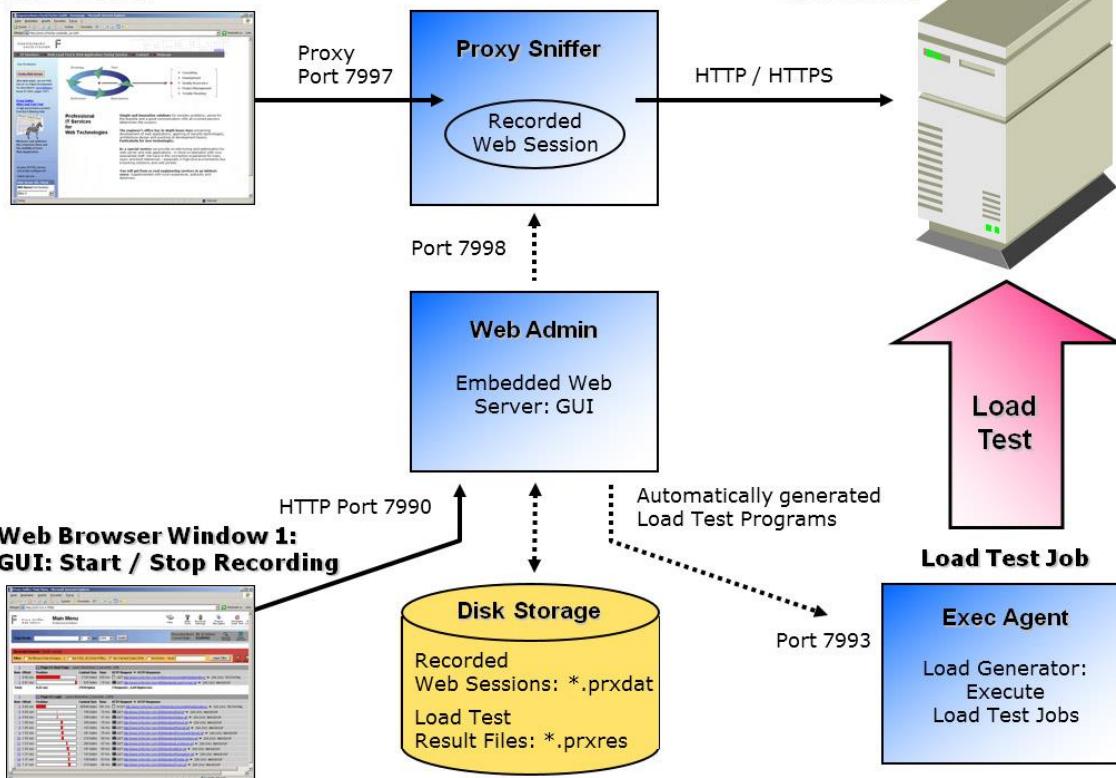
[Generating an own, private CA Root Certificate on Linux](#)

[Appendix A: Import your CA Root Certificate into an Apple iOS device \(iPhone and iPad\)](#)

2 Architecture Overview

2.1.1 Local Architecture

Web Browser Window 2: Web Session



ZebraTester contains four built-in server components which are started on your local computer:

- Proxy Sniffer**: A special proxy server used to record Web surfing sessions.
- Web Admin**: An embedded, local Web server for the GUI.
- Exec Agent**: A server which supports the execution of load test jobs.
- Job Controller**: A server which allows to combine several load-releasing machines into a cluster.

The following TCP/IP server ports have been set up on your local system:

TCP/IP Port Number	Port Description
7990	Embedded Web Server, GUI (Web Admin)
7993	Load Test Execution Server (Exec Agent)
7995	Load Test Cluster Controller (Job Controller)
7996 (optional)	REST API Server (Proxy Sniffer)
7998	Internal communication port (Proxy Sniffer)
7997	HTTP/S Proxy Port (Proxy Sniffer)
7999 (deprecated)	HTTP Proxy Port, HTTP only (Proxy Sniffer)

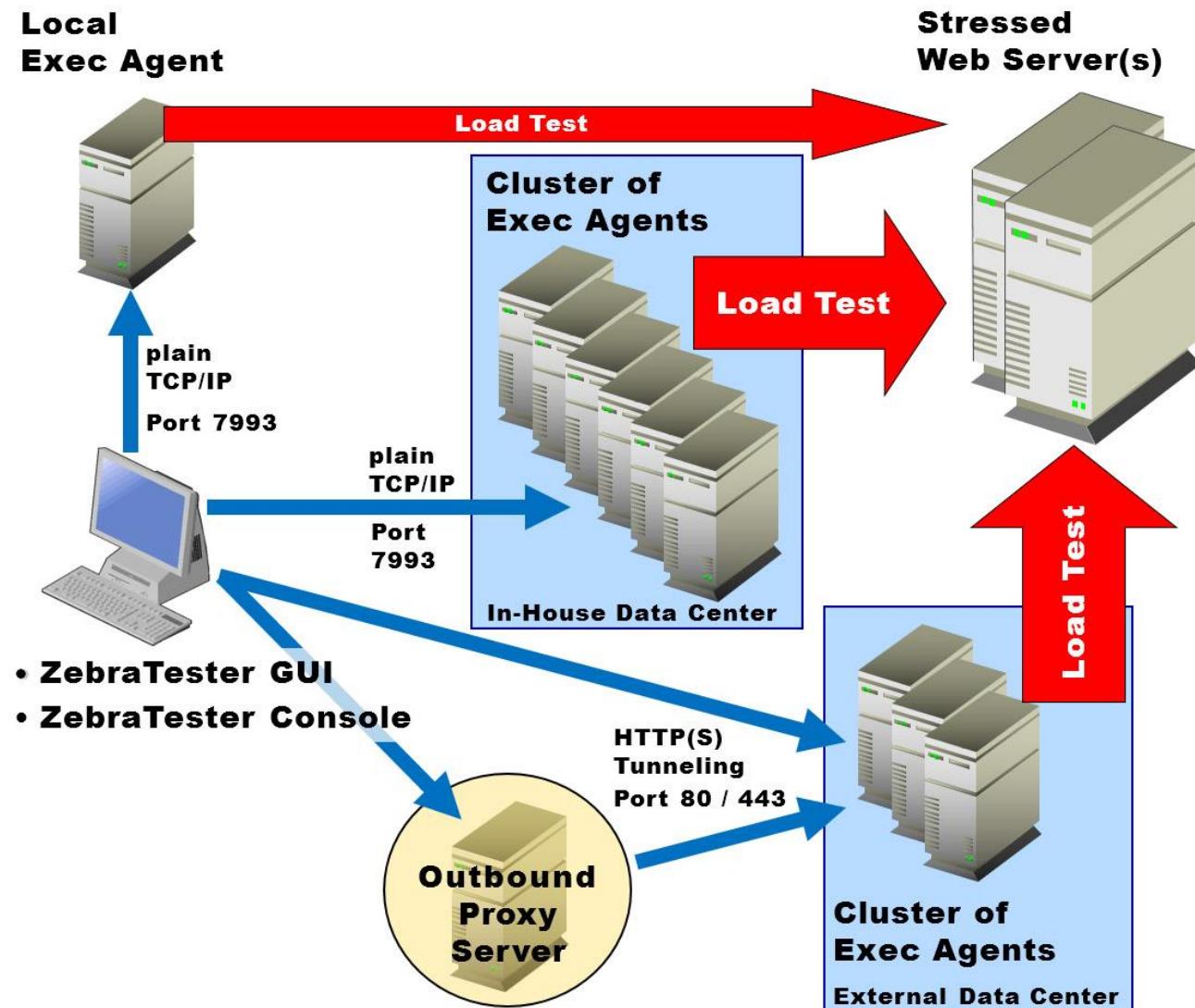
Note: The **ZebraTester Console** application execute all of these four server components as integrated threads.

2.1.2 Distributed Architecture

Remote execution of load tests, as well as combining several Exec Agents (load generators) to a load generating cluster, is supported in an easy and transparent way.

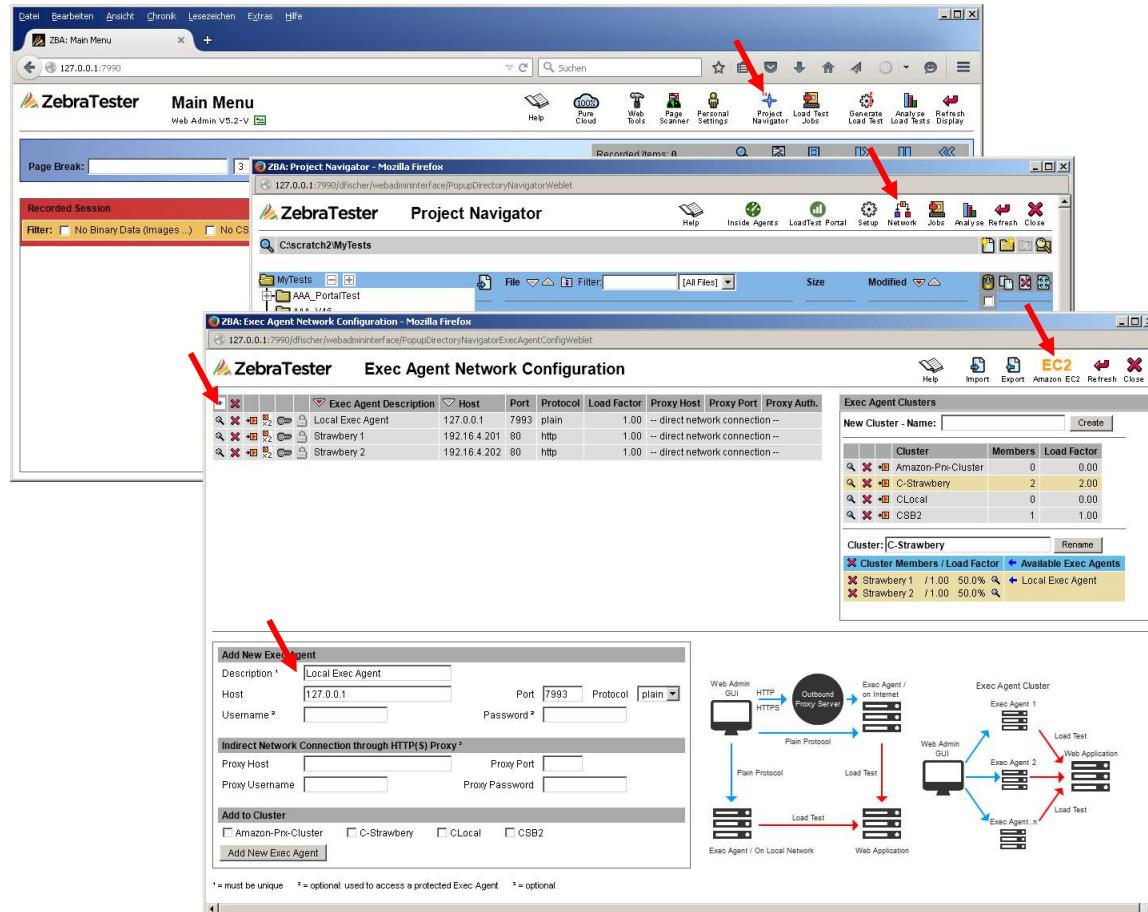
On remote systems normally only Exec Agent are installed and started. They are normally running on port 7993 when plain TCP/IP connections are used or on Port 80 or 443 when HTTP/S connections are used for the internal ZebraTester communication between your local system and the remote Exec Agents – but any other TCP/IP port can also be configured. **Please note that you have to enable the corresponding inbound firewall rule on the remote systems.**

Further information about starting Exec Agents as a **Windows Service** or as a **Unix Daemon** is available in the **Application Reference Manual**.



2.1.2.1 Configuring Additional Load Generators (Exec Agents)

An Exec Agent is already started on your local system as part of the ZebraTester Console. Additional Exec Agents – which run on remote systems – can be defined in the **Exec Agent Network Configuration** menu, which is reachable from Main Menu → Project Navigator → Network:



HTTP/S proxy server means, in this case, that load tests can be started from a protected corporate network, to any load releasing systems on the internet – all without the need for ordering new firewall rules.

Hint: you can test the configuration and the accessibility of an Exec Agent by clicking on the icon within the list of Exec Agents (functional “ping” of the Exec Agent).

Additional Exec Agents which are running in your local network can be added in the lower part of the window.

Optionally, pre-installed Exec Agents which are running in the **Amazon Cloud** can be added by clicking on the EC2 icon in the upper right corner of the window. Such Exec Agents can be instantly rented per hour, or can be accessed by purchasing an "Unlimited Exec Agent Weekly License".

Several Exec Agents can be combined to a load-generating cluster. This can be done by using the **Exec Agent Clusters** dialogue at the right side of the window.

The operating system of the machines in a load-generating cluster (the cluster members) can also be heterogeneous; that is, Windows and Unix-like systems, as well as strong and weak systems, can be mixed within the same cluster. The individual cluster members can be placed in different locations, and can also use different protocols to communicate with the Web Admin GUI.

The communication between the Web Admin GUI and the remote Exec Agent processes usually uses raw TCP/IP network connections to port 7993; however, this port number can be freely chosen if an Exec Agent process is installed separately. The communication can also be made over HTTP or HTTPS connections (tunneling), and also supports outbound HTTP/S proxy servers. The support of outbound

2.2 Protecting the Web Admin GUI from Unauthorized Remote Access

By default there is no protection configured against accessing the Web Admin GUI from remote systems (i.e. by starting a Web browser on any system and entering <http://<ZebraTester-GUI-Host>:7990> into the browser). But you can enable the remote access protection which effects that each person who accesses the Web Admin GUI from a remote system must enter first a valid username and password to get access to the Web Admin GUI.

Note: OS users which have access to the local machine on which the Web Admin GUI is started, and are using a Web browser on this local machine - never require a username and password to access the Web Admin GUI. Therefore keep in mind that the Web Admin GUI can be protected only against unauthorized remote access – but not against unauthorized local access.

2.2.1 Enabling the Remote Access Protection

Proceed as follows:

1. Open a ZebraTester Command terminal:
 - a. On Windows: Click on Start ▶ All Programs ▶ ZebraTester ▶ **ZebraTester Command Prompt**
 - b. On Mac OS X: Open a Finder window ▶ Navigate to the ZebraTester installation directory ▶ Click on **ZebraTesterCommand.command**
 - c. On Linux: Open a File Manager window ▶ Navigate to the ZebraTester installation directory ▶ Click on **ZebraTesterCommand.desktop**
2. Enter in the terminal: **java WebAdminLoginAccounts**
3. Create a super user "Web GUI account" by calling the menu option 7 (add account)

After entering **java WebAdminLoginAccounts** you see the following menu:

```
Web Admin GUI protected = false

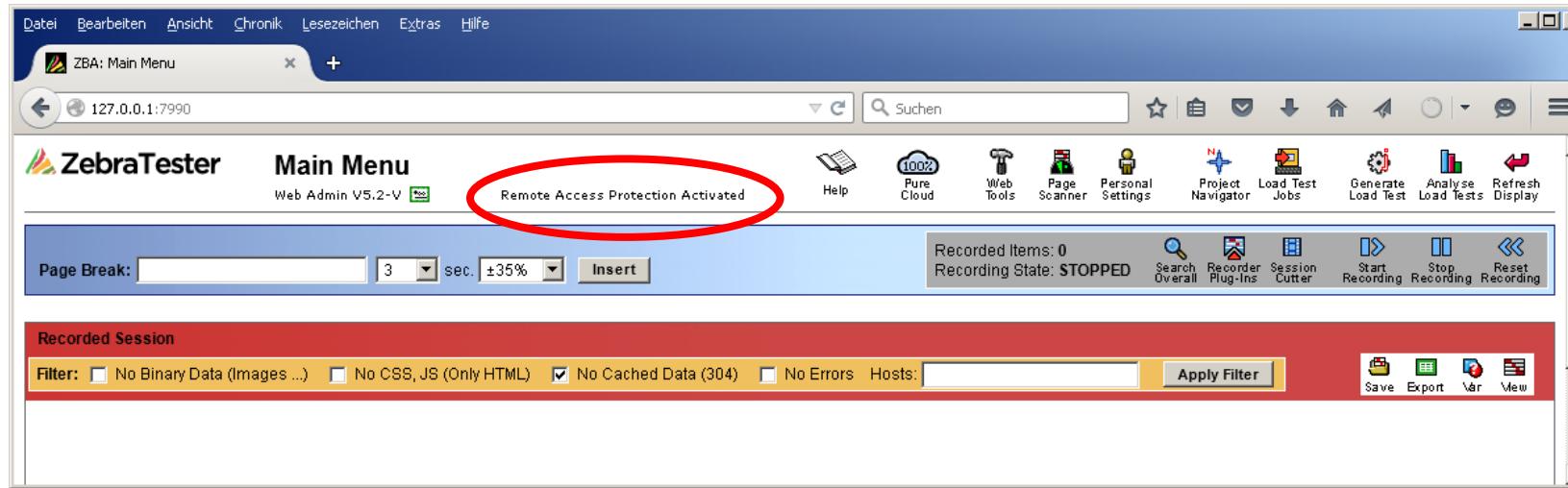
1 = list all accounts
2 = reset password
3 = enable account
4 = disable account
5 = set superuser
6 = remove superuser
7 = add account
8 = delete account
9 = delete file WebAdminLoginAccounts.dat - disable any protection and delete all accounts

0 = exit

select =
```

Enter now 7 and create a new super user account. Then exit this utility.

- After that start a Web browser on the local machine where the Web Admin GUI is installed and call the Web Admin menu by entering <http://127.0.0.1:7990> into the Web browser. You should see now a hint showing you that the Remote Access Protection is enabled:



- On any other system, start a Web browser and enter <http://<ZebraTester-GUI-Host>:7990> into the browser. Then you will see a login form. Enter the username and the password of the super user into the form:



3. You can now **create additional accounts** and manage them remotely. However, keep in mind that internal context of the Web Admin GUI only supports to be operated by one "natural" user at the same time:

The image shows two screenshots of the ZebraTester Web Admin interface.

Main Menu Screenshot: The top screenshot shows the ZebraTester Main Menu. A red arrow points to the "Logout" button, which has the username "miller" written above it. The menu bar includes "Datei", "Bearbeiten", "Ansicht", "Favoriten", "Extras", and "?". The toolbar contains icons for Help, Pure Cloud, Web Tools, Page Scanner, Personal Settings, Project Navigator, Load Test Jobs, Generate Load Test, Analyse Load Tests, and Refresh Display. Below the toolbar, there are controls for "Page Break" (3 sec. ±35%) and "Recorded Items: 0 Recording State: STOPPED". Buttons for "Search Overall", "Recorder Plug-Ins", "Session Cutter", "Start Recording", "Stop Recording", and "Reset Recording" are also present. A "Recorded Session" section with a filter for "No Cached Data (304)" is shown, along with "Save", "Export", "Var", and "View" buttons. The status bar at the bottom indicates "100%".

Manage Login Account Screenshot: The bottom screenshot shows the "Manage Web Admin Login Account" page. A red arrow points to the "+" button in the top-left corner of the table header. The table displays a single account entry:

	Username	Enabled	Superuser	Last Login Date (ECT)	Last Login Remote IP
	miller	yes	yes	03 Jul 2015 23:41:05	192.16.4.160

The page includes a "Help" button and "Refresh" and "Close" links in the top right.

4. **Note:** If a logged in user does not have super user privileges the functionality of this menu is restricted, and allows to change only the own password.

The screenshot shows a web browser window titled "ZBA: Manage Login Account - Internet Explorer". The URL in the address bar is "http://192.16.4.13:7990/dfischer/webadmininterface/WebAdminManageLoginAccountWeblet". The main title is "Manage Web Admin Login Account". On the left, there is a section titled "Account meier" with the following details:

Superuser	no
Last Login Date (ECT)	03 Jul 2015 23:48:34
Last Login Remote IP	192.16.4.160

Below this, there are fields for changing a password:

Set New Password Old Password:
 New Password:

A "Set New Password" button is located at the bottom left of the form area.

3 Reconfiguring the Web Browser for the Recording of Web Surfing Sessions

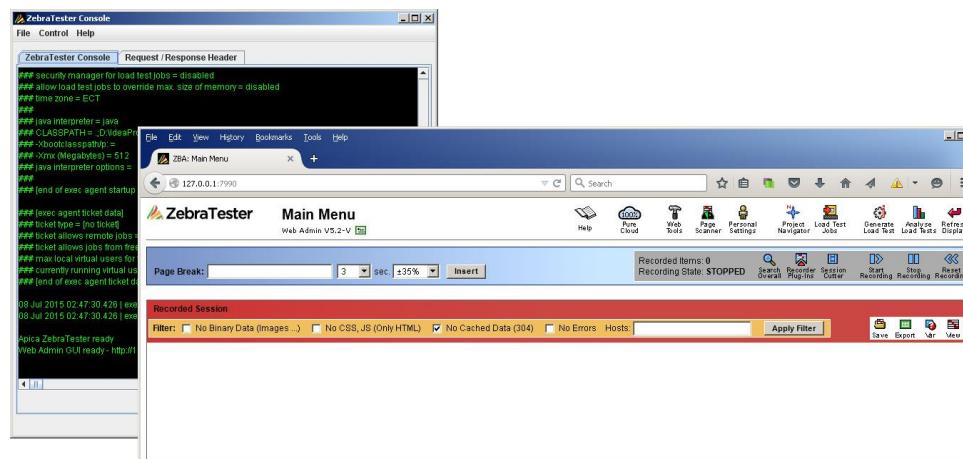
Note: You can skip this chapter if you are using a **Firefox Web Browser** for the recording of Web surfing sessions. In such a case download the **Firefox Recording Extension** from http://www.zebratester.ch/download/zebratester_recording_extension-3.4003-fx.zip (unzip the content to a local folder after download). Note that you should also import your own created ZebraTester/ProxySniffer CA Root Certificate **root.cer** into Firefox.

Click on the  icon inside the **ZebraTester Toolbar** and follow the instructions:



Recording of Web surfing sessions is supported by using any Web browser, such as **Internet Explorer**, **Google Chrome** or **Safari**. You can also use Firefox without installing the Firefox Recording Extension. And you can record also the HTTP/S traffic of any (technical) Web Client Application.

After you have installed and started the **ZebraTester Console**, and entered <http://127.0.0.1:7990> in your Web browser – or clicked on the **ZebraTester GUI** icon, you will see the Main Menu (shown below). This GUI is also referred to as **Web Admin**.



Before using ZebraTester, you must configure appropriate Web browser settings:

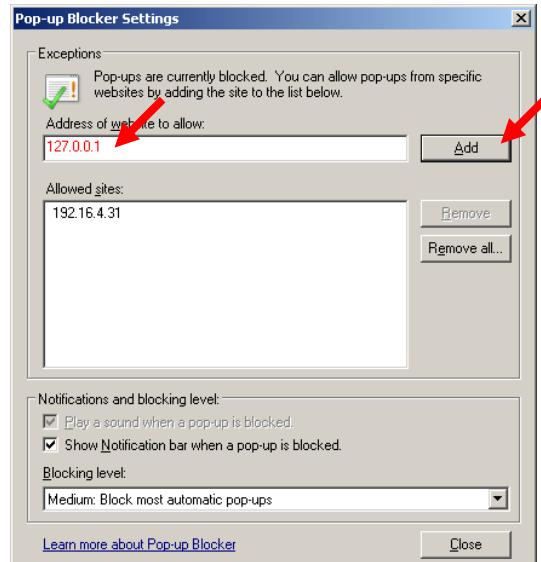
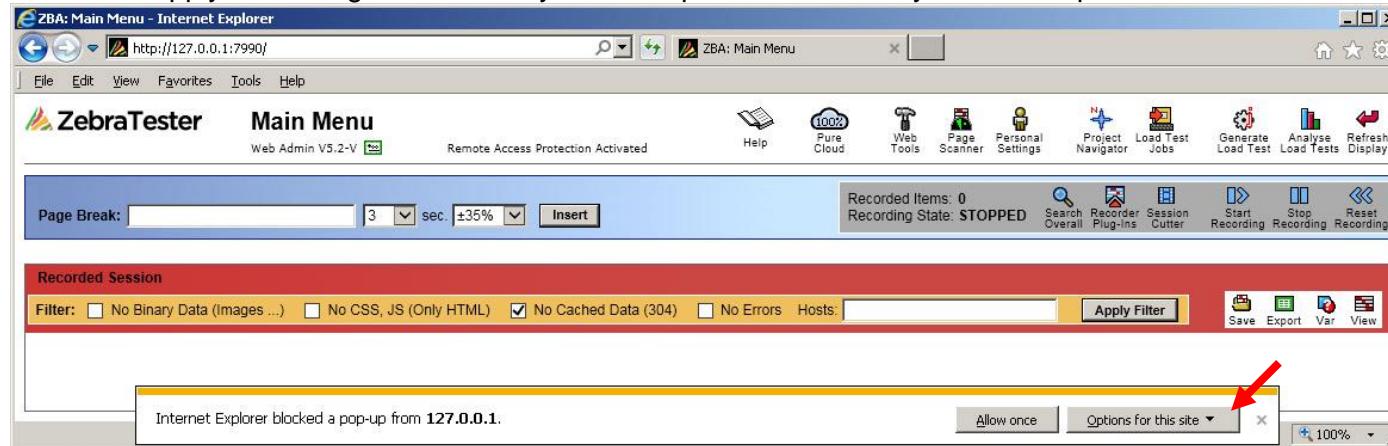
- Pop-up windows must be allowed from the local host (127.0.0.1)
- A special, local proxy server is already started with the product. Recording web surfing sessions requires that the data exchange between the Web browser and the Web server(s) flows through this local proxy server; therefore, the Web browser must be re-configured for recording.

These two activities are now described in detail.

3.1 Enabling Pop-up Windows from Local Host

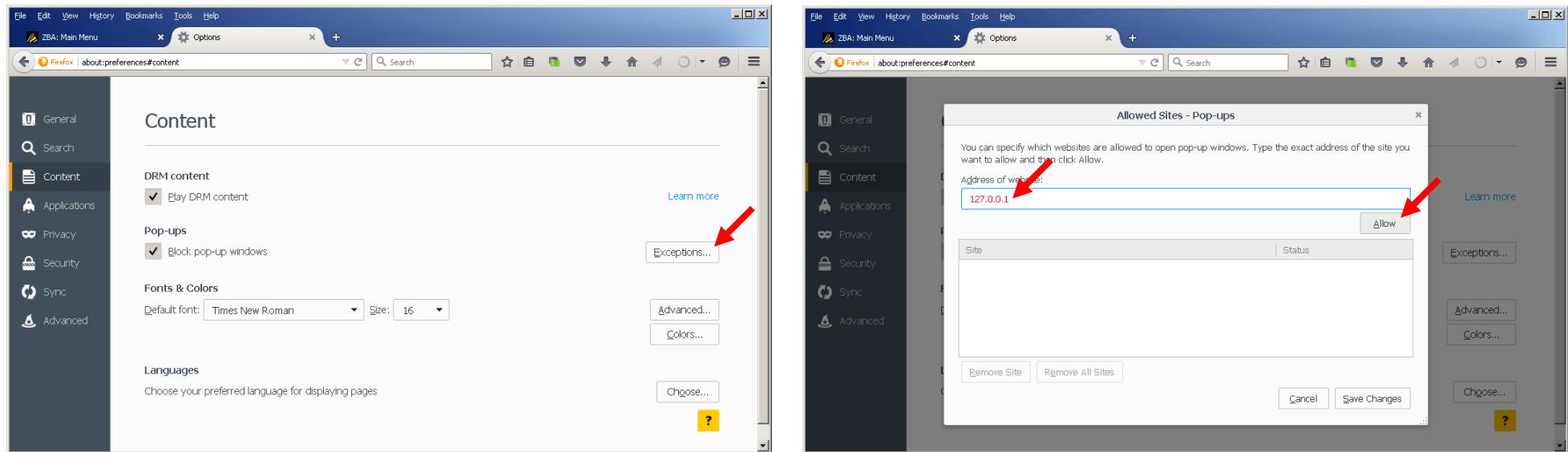
You must configure the Web browser to allow pop-up windows from the local host 127.0.0.1 (the IP loopback address of your own host). This is not a security problem because pop-up windows from all other hosts, such as Internet Web sites, are still blocked.

The following screenshots show how to enable local host pop-up windows for **Microsoft Internet Explorer**. Use the address of the loopback interface **127.0.0.1**. Apply this configuration when you are requested to do so by Internet Explorer.

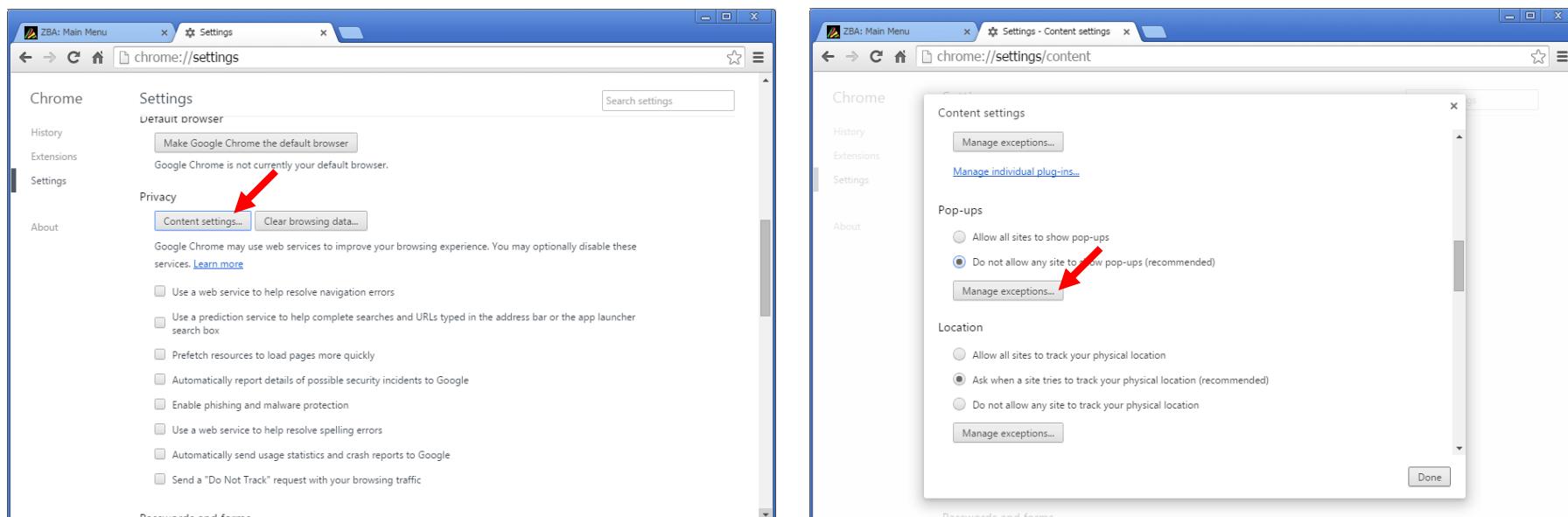


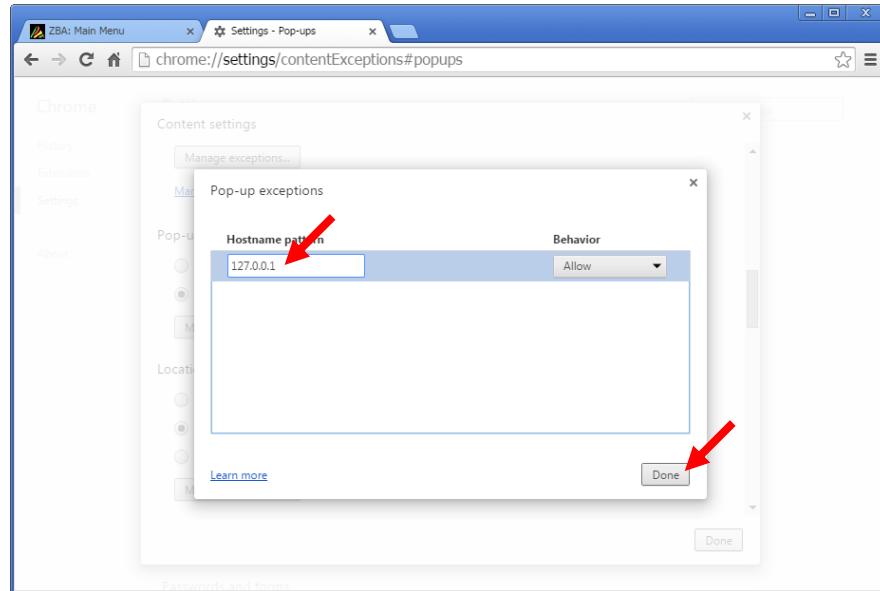
Alternatively, you can also call the pop-up blocker configuration dialog direct from the **Internet Options** → **Privacy** menu.

The following screenshots show how to enable local host pop-up windows for **Firefox**, released from the Web Admin GUI on your own computer:

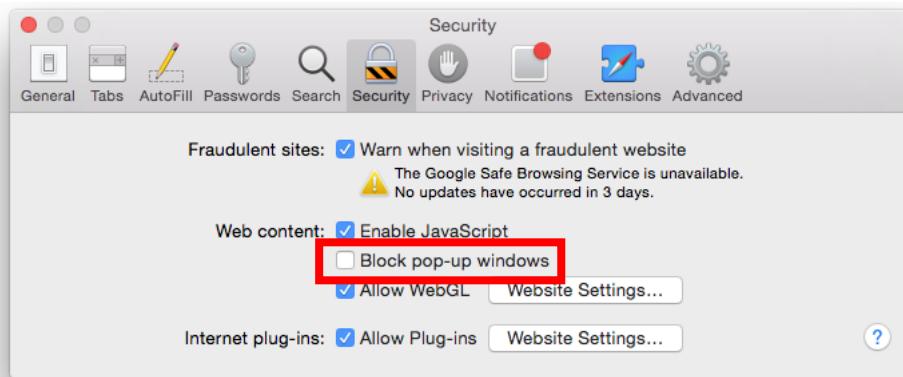


The following screenshots show how to enable local host pop-up windows for **Google Chrome**:





The following screenshot show how to enable pop-up windows for **Safari**:



Hint: If you have installed **Google Toolbar**, you must also configure or deactivate the toolbar's pop-up blocker.

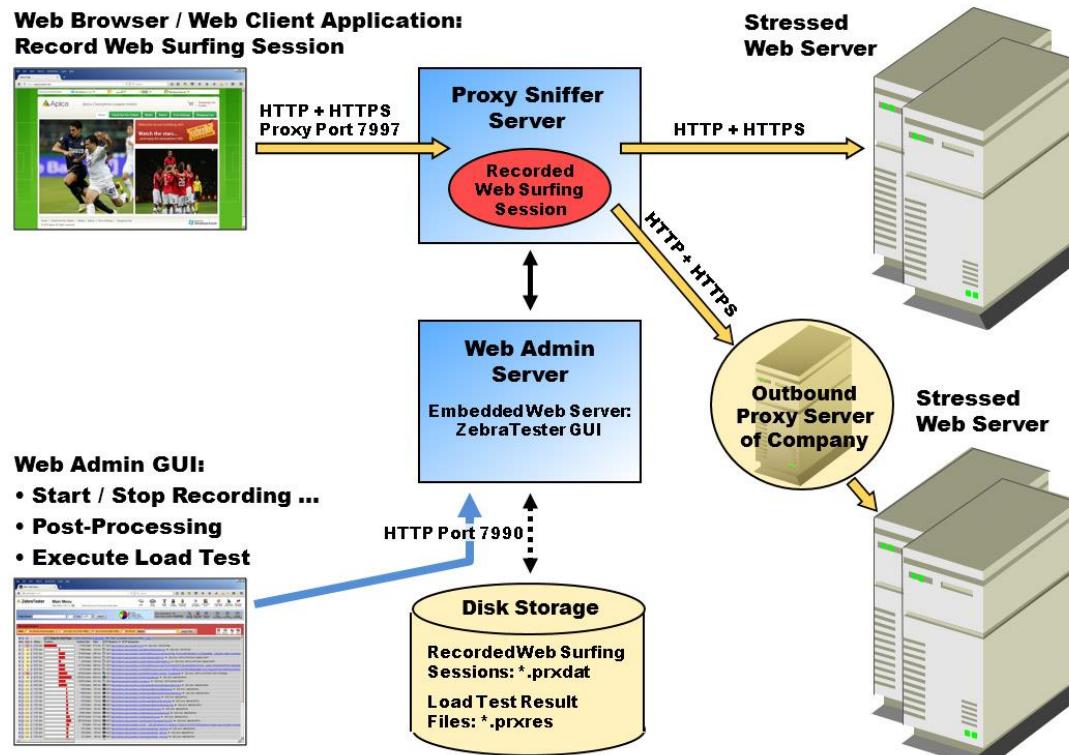
3.2 Reconfiguring a Web Browser for Recording

You must reconfigure a Web browser to use ZebraTester for recording Web surfing sessions. This means that the Web browser must be reconfigured in such a way, that the HTTP/S traffic flows over the local Proxy 127.0.0.1 by using the TCP/IP port 7997.

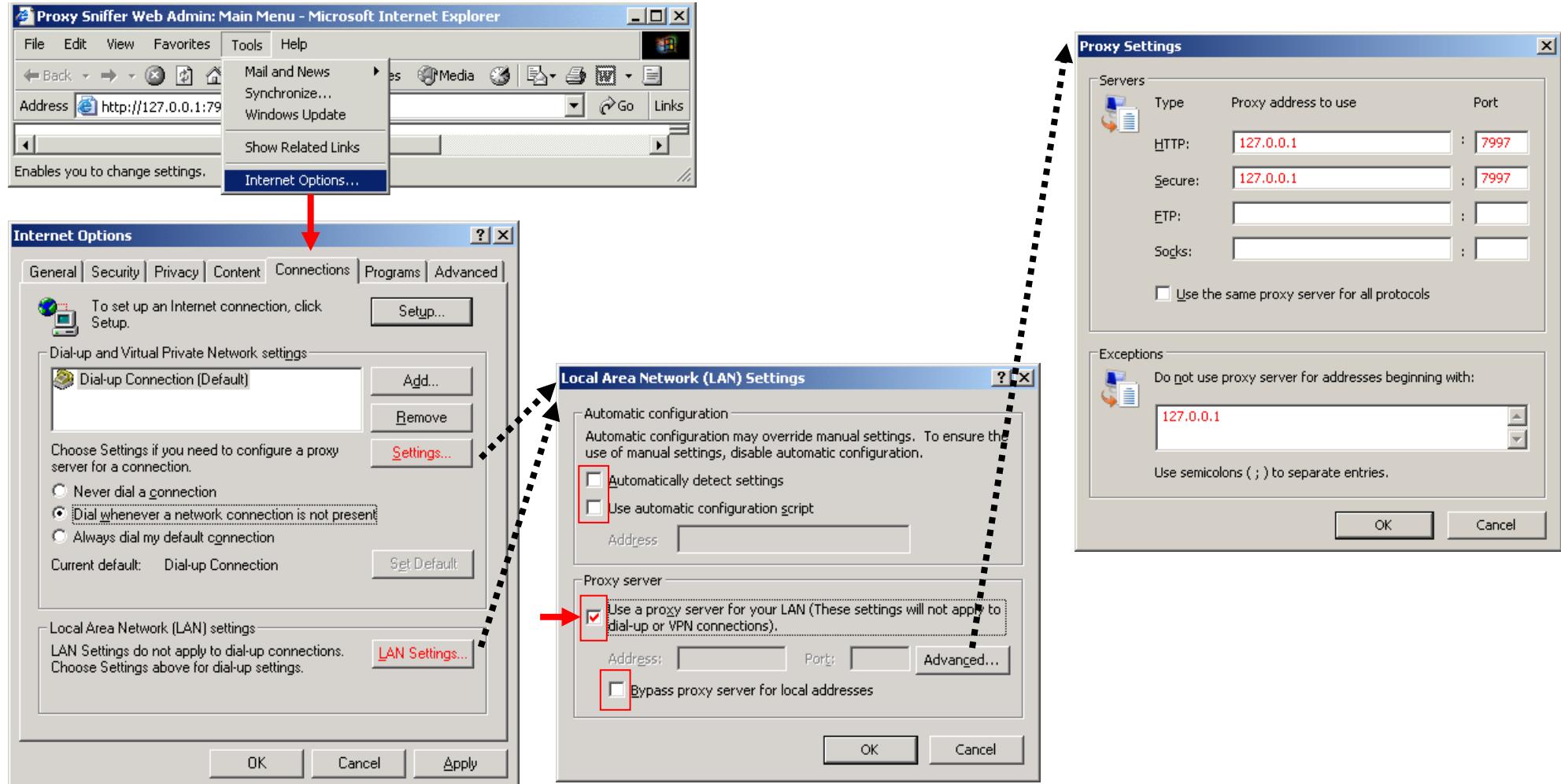
You can use the same Web browser product for recording load tests and for using the Web Admin GUI, or you can use two different Web browser products – one for recording load tests and another for the Web Admin GUI.

If you use only one Web browser product for recording and for the Web Admin GUI, you must exclude your localhost 127.0.0.1 from the Web browser proxy configuration because the usage of the (local) embedded Web Admin Server must not flow into the recorded Web surfing session.

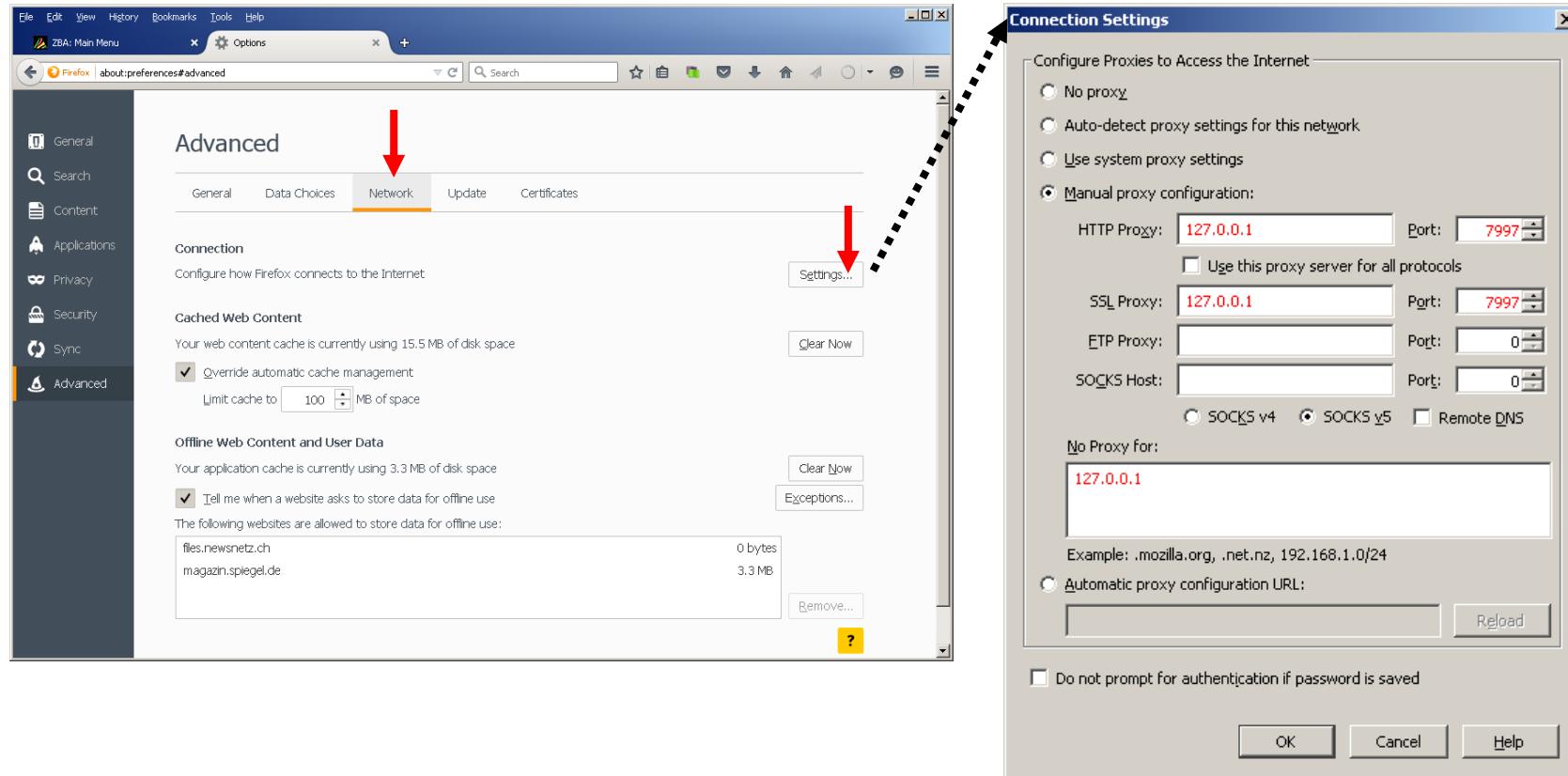
Hint: You should undo this special Web browser proxy configuration after the successful recording of a Web surfing session, in order that you can surf again without ZebraTester. **The proxy configuration of the Web browser is not needed for the execution of load tests (recording only).**



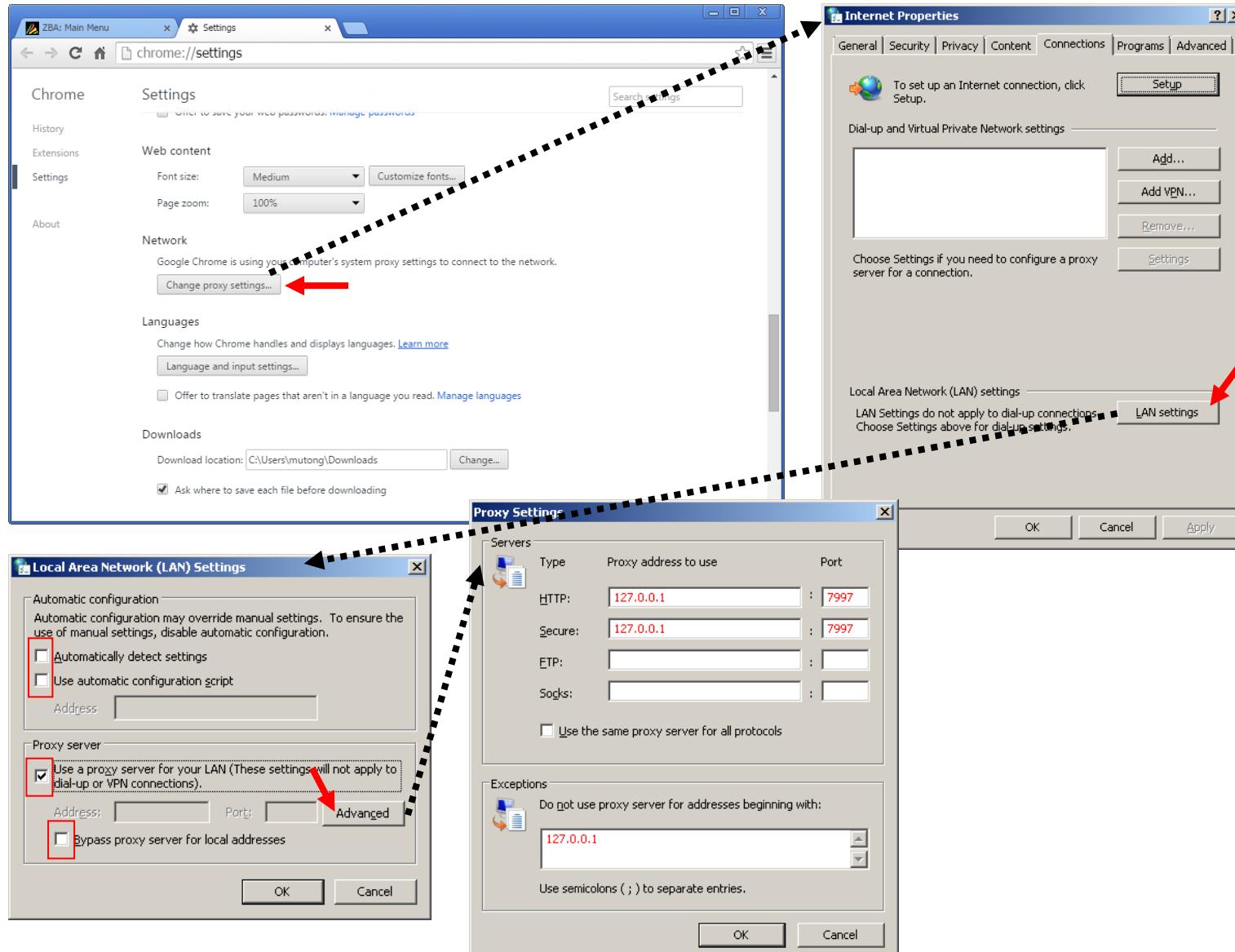
3.2.1 Microsoft Internet Explorer Proxy Configuration



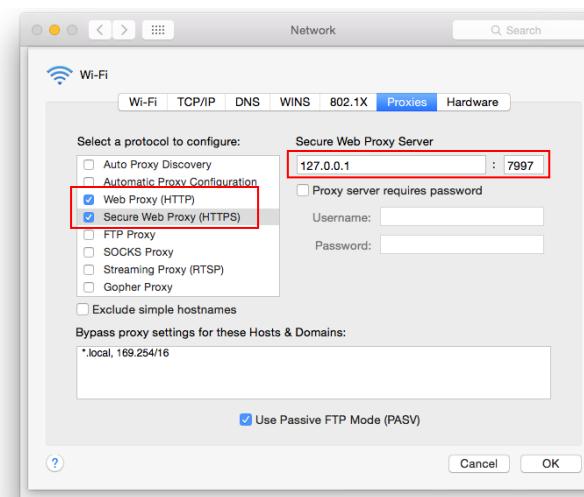
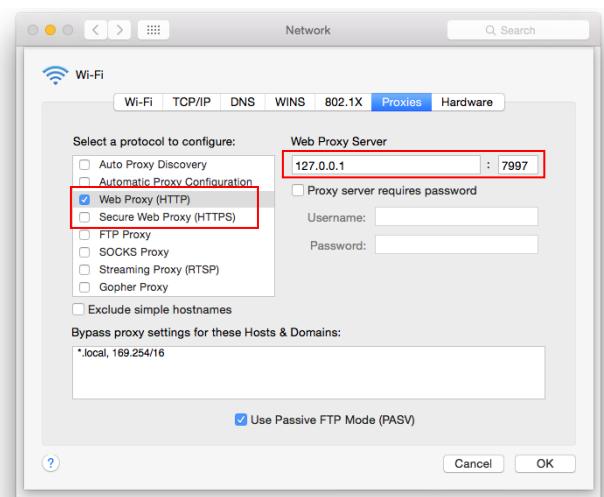
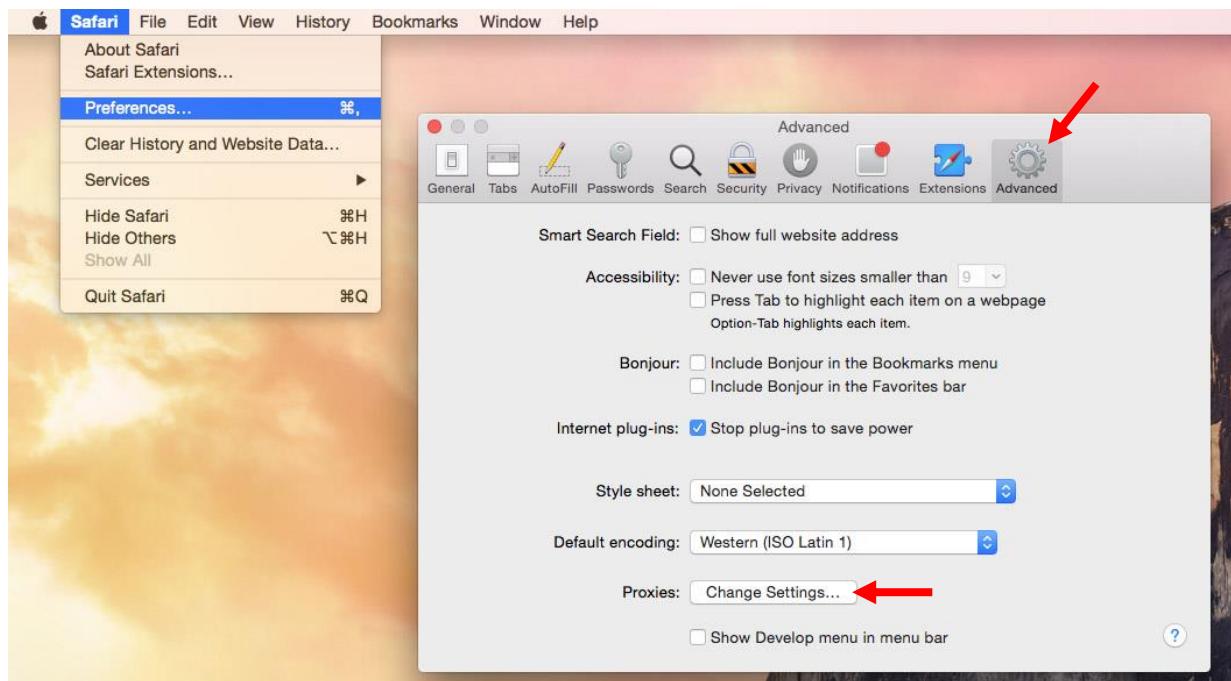
3.2.2 Firefox Proxy Configuration



3.2.3 Google Chrome Proxy Configuration



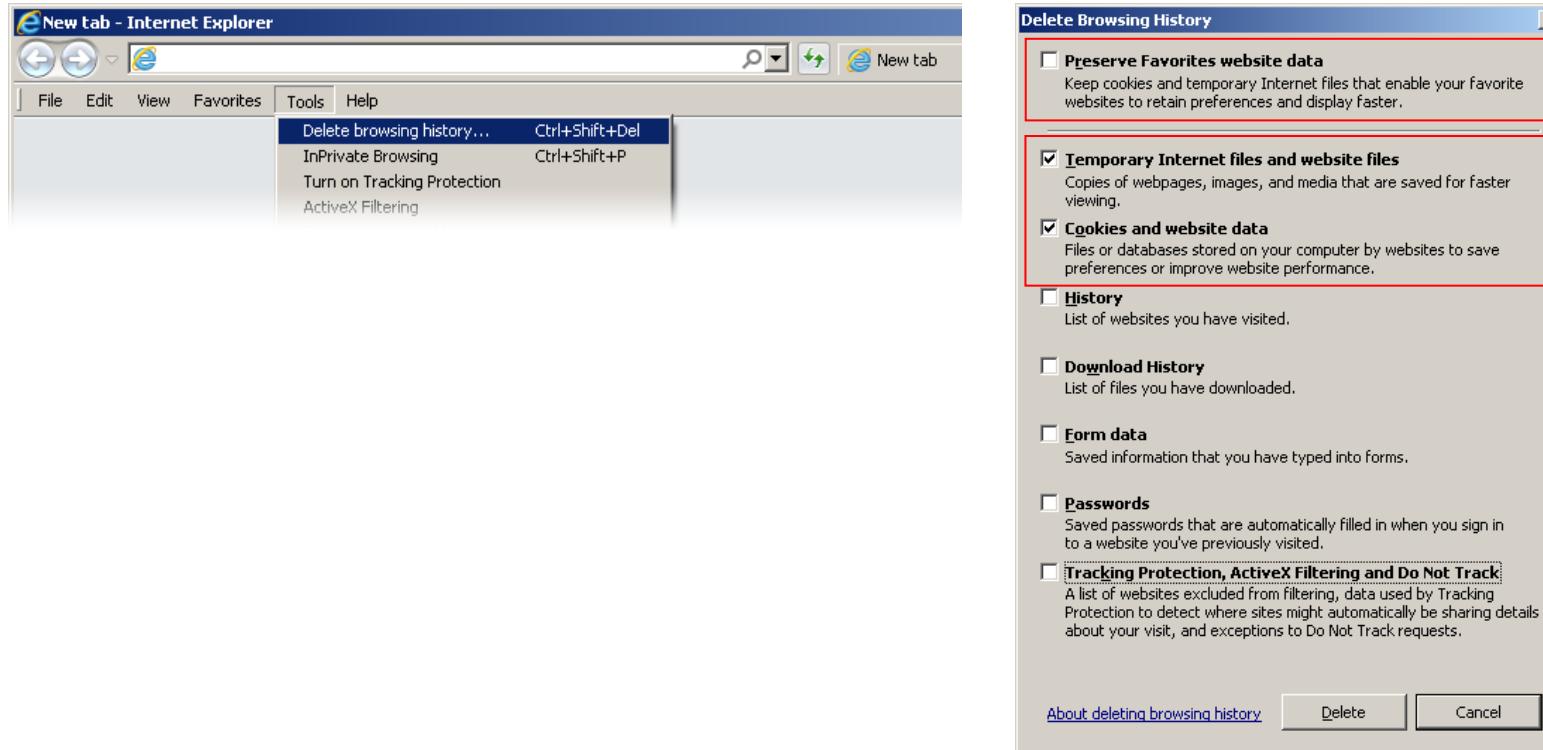
3.2.4 Safari Proxy Configuration



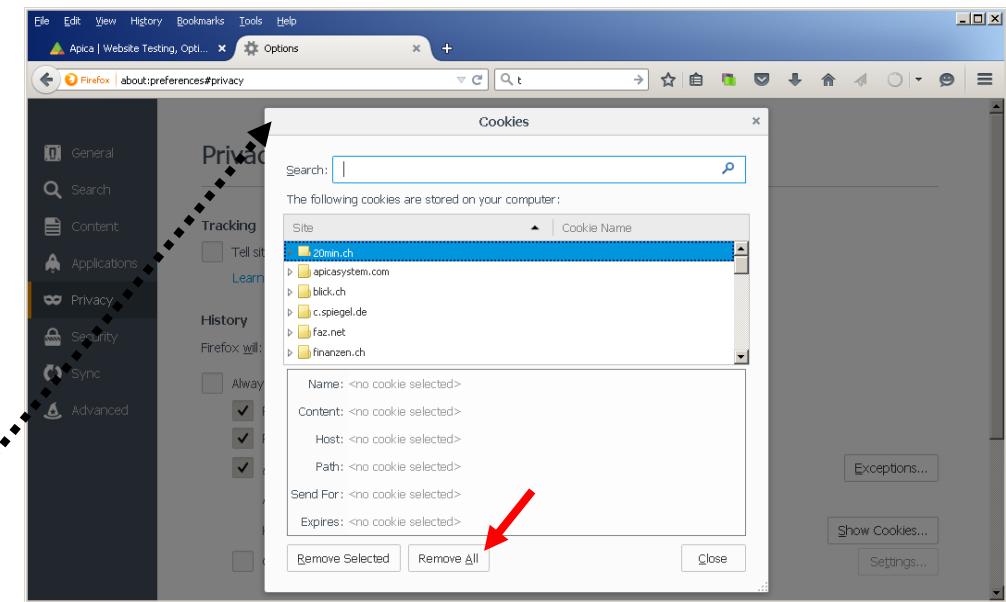
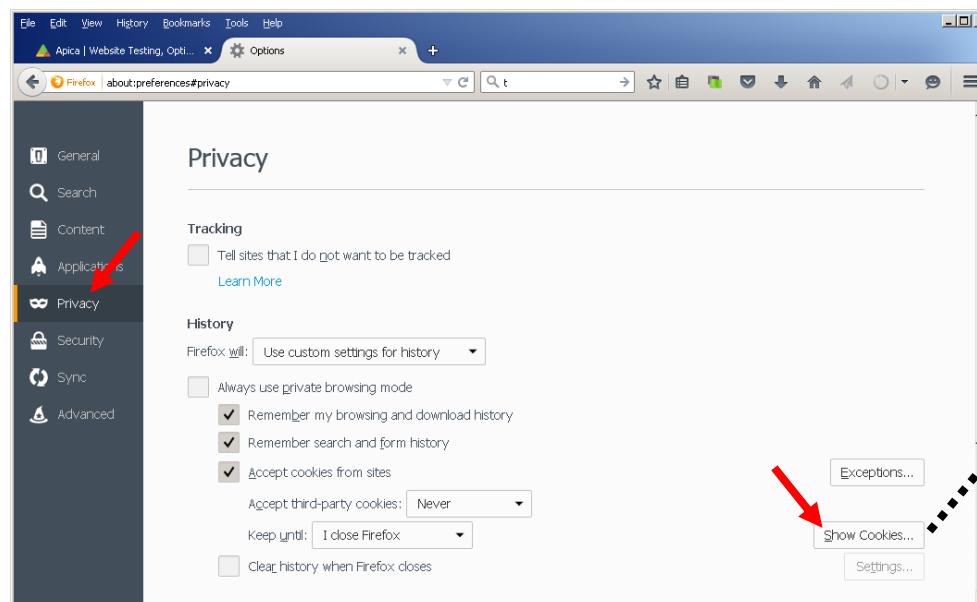
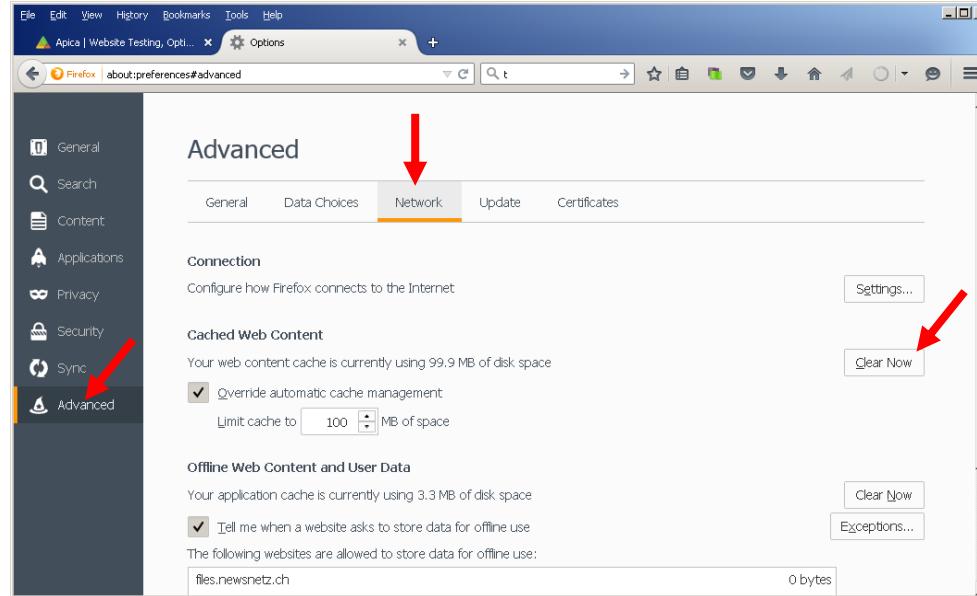
3.3 Clearing the Web Browser Cache and all Cookies every time before Recording

Please note that you must first **clear the Web browser cache and all cookies every time before you start recording a new Web surfing session.**

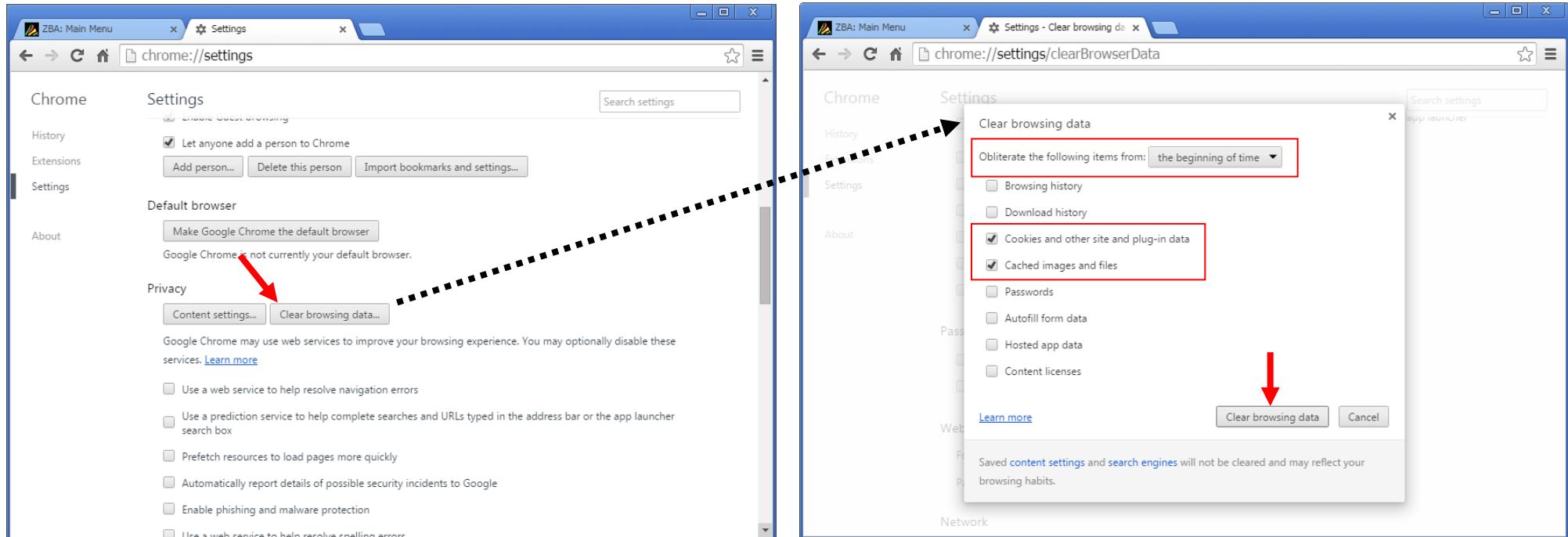
3.3.1 Internet Explorer / Clearing Cache and Cookies



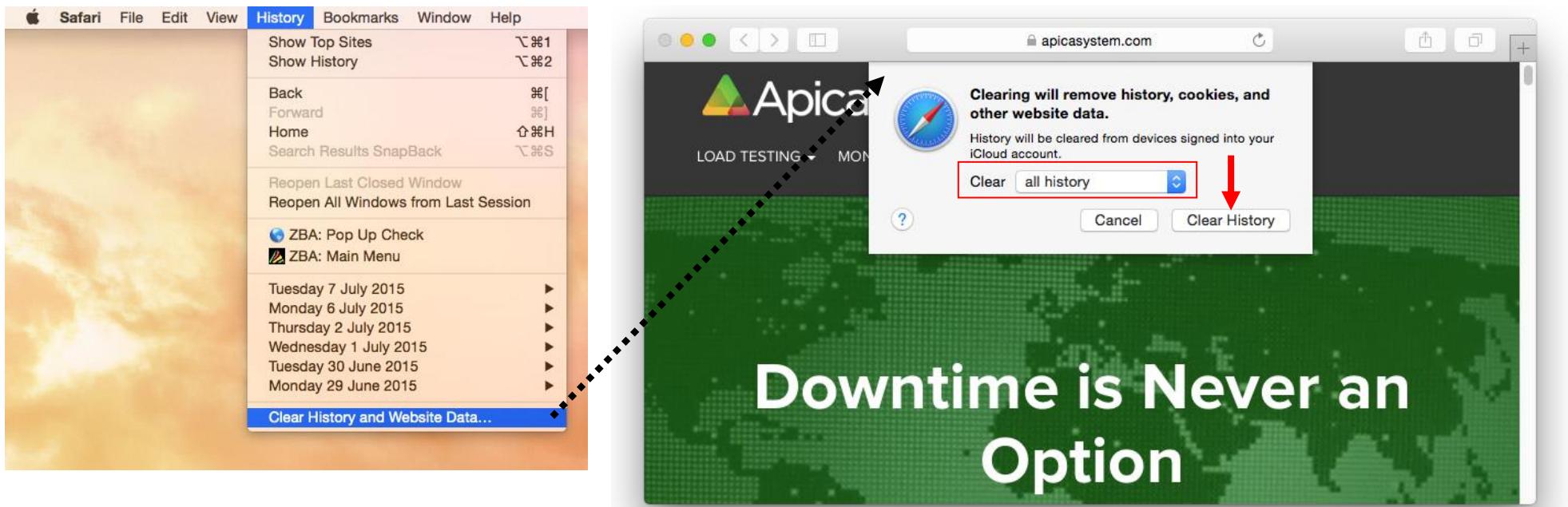
3.3.2 Firefox / Clearing Cache and Cookies



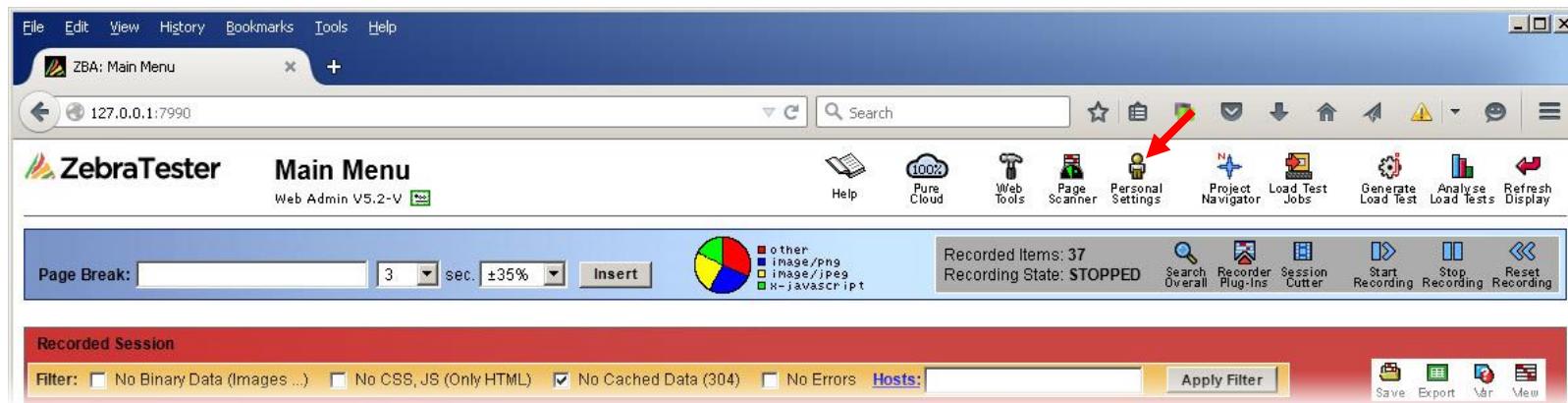
3.3.3 Google Chrome / Clearing Cache and Cookies



3.3.4 Safari / Clearing Cache and Cookies

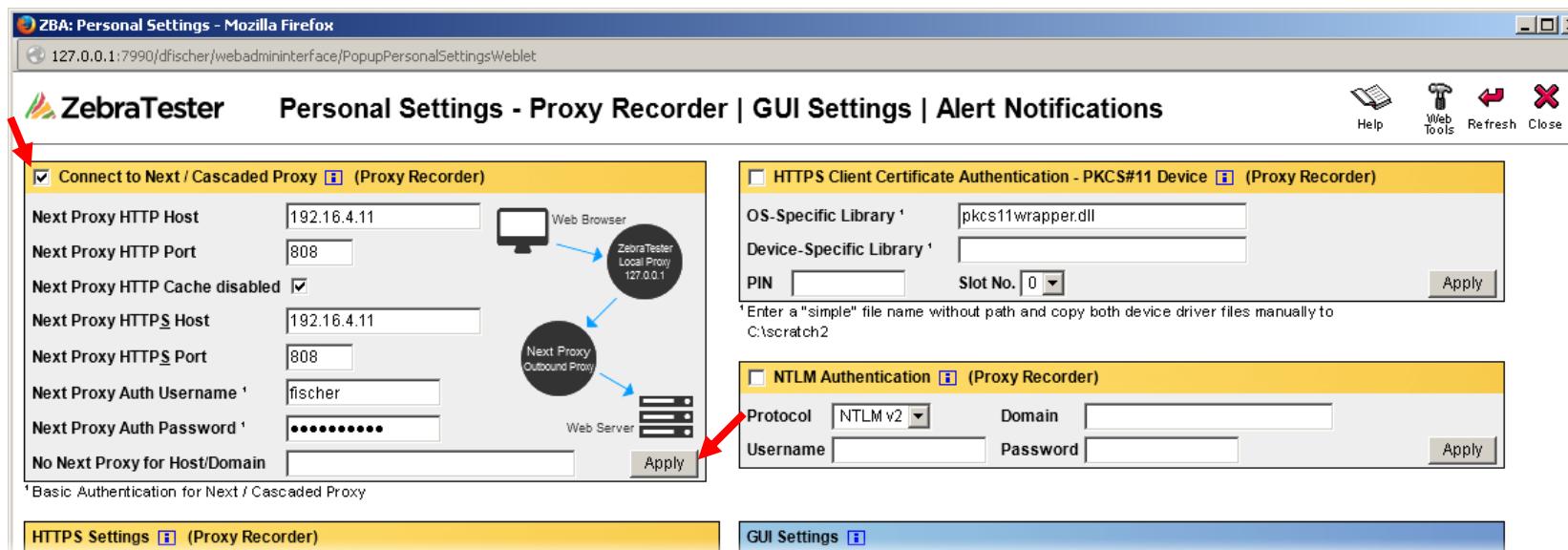


3.4 Recording via an Outbound Proxy Server of your Company



Cascading ZebraTester with an outbound proxy server of your company is supported as an optional configuration. Use this option if you only have an indirect network connection from your local workstation (located inside a corporate network), over an outbound proxy server, to the external stressed

Web server. The outbound (cascaded) proxy server can be configured in the Personal Settings menu which is accessible from the main menu.



However, consider that **the execution of load tests via an outbound proxy of your company is not recommended** because the measured test results may be wrong and because the outbound proxy server may crash. We recommend to use the outbound proxy server for recording purposes only, and to execute the load test in such a case from the Apica Load Test Portal (LTP), or from Amazon EC2 load generators.

Appendix A: Import your CA Root Certificate into an Apple iOS device (iPhone and iPad)

To record sessions from iOS devices such as iPhone and iPad you have to install your self-generated CA root certificate on these devices. You can **e-mail your CA root certificate** to an Apple iOS device, or alternatively **put it on any Web server** and address its URL directly in Safari. After clicking on the certificate in the e-mail, or entering the URL in Safari, your CA root certificate can be imported:

