Security Hint: Please read at least chapter 1.7 in this document. Do not import the common CA Root Certificate delivered by the Proxy Sniffer installation kit (file: root.cer) into your OS or Web browser.
## 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 Further Hints for using Proxy Sniffer on Windows - Firefox Portable and Firefox Recording Extension .................................................................................................................. 6
    1.3.2 Windows System Tuning ................................................................................................. 8
      1.3.2.1 Disabling HTTP/S Anti-Virus Network-Scanning .................................................. 8
      1.3.2.2 Windows XP .......................................................................................................... 9
      1.3.2.3 Windows 2003 Server ............................................................................................ 9
      1.3.2.4 Windows 7 and Windows 2008 Server ................................................................... 9
  1.4 Installation on Mac OS X ......................................................................................................... 10
    1.4.1 Mac OS X System Tuning ............................................................................................... 11
    1.4.2 Mac OS X Java Modification / Edit java.security ....................................................... 12
    1.4.3 Special Instructions for Mac OS X 10.9 (or newer) / Prevent "App Nap" ....................... 13
    1.4.4 Special Instructions for Java 7 on Mac OS X 10.8 (or newer) .................................... 14
  1.5 Installation on Ubuntu (Linux) ............................................................................................... 17
  1.6 Installation on all other Unix-like Systems (Linux, Solaris, BSD ...) .................................... 22
    1.6.1 Unix-Like System Tuning (Solaris, Linux, BSD ...) ..................................................... 23
  1.7 Post Installation / Security Hint for all Operating Systems .................................................. 24
  2 Architecture Overview .............................................................................................................. 25
    2.1.1 Local Architecture ......................................................................................................... 25
    2.1.2 Distributed Architecture ............................................................................................... 27
      2.1.2.1 Configuring Additional Load Generators (Exec Agents) ...................................... 28
    2.2 Protecting the Web Admin GUI from Unauthorized Remote Access ............................ 29
      2.2.1 Enabling the Remote Access Protection .................................................................... 29
  3 Reconfiguring the Web Browser for Recording of Web Surfing Sessions ................................. 33
    3.1 Enabling Pop-up Windows from Local Host ..................................................................... 34
    3.2 JavaScript Settings for Firefox ......................................................................................... 35
    3.3 Reconfiguring a Web Browser for Recording .................................................................... 36
      3.3.1 Microsoft Internet Explorer Proxy Configuration ...................................................... 37
      3.3.2 Firefox Proxy Configuration ....................................................................................... 38
      3.3.3 Safari Proxy Configuration ......................................................................................... 38
      3.3.4 Web Browser Warning Messages (HTTPS) ............................................................. 39
    3.4 Clearing the Web Browser Cache and all Cookies every time before Recording ............... 40
  4 Next Steps for Recording Web Surfing Sessions and Executing Load Tests ............................ 41
  Appendix A: How to create your own CA Root Certificate on Windows Systems .................. 42
  Appendix B: Import your CA Root Certificate into an Apple iOS device (iPhone and iPad) .... 45
1 Installation

Administrator or root user privileges may be required for the installation of Proxy Sniffer, but normally administrator rights are not required when installing Proxy Sniffer in the suggested default location. In addition, after installation, Proxy Sniffer requires write access to its own installation directory and to the associated sub-directories.

1.1 System Requirements

- Supported operating systems: Windows XP/Vista/7/2003/2008 or Unix-like systems: Solaris, Linux, Mac OS X …
- RAM: 4096 MB recommended, minimum 2048 MB. Windows 64-Bit installation kit used for high-duty load generators only: minimum 16 GB, 24 GB recommended.
- GUI: minimum recommended screen resolution: 1280 x 800 pixels
- 250 MB free disk space
- On UNIX-like systems (only): a Java SDK (Java Software Development Kit) 1.6 (Java version 6) must be pre-installed ¹
- Adobe Reader to display PDF files

¹ On Mac OS X, Java is already pre-installed. For all other UNIX-like systems: the successful operation of Proxy Sniffer requires that you install the original SDK implementation from SUN Microsystems (Oracle) – all other SDK implementations are not supported.

For Windows systems, an own Java 1.6 compiler and interpreter is already bundled with the Proxy Sniffer Windows installation kit. The installed Java SDK of Proxy Sniffer does not tamper any other Java installations on your Windows system.

1.2 Recommendations for Load Generators (Exec Agents)

We recommend to use 64-Bit operating systems as Load Generators (for example Linux-Ubuntu, Solaris or Windows 2008) and to use/install the official JAVA 1.6 (Java 6) 64-Bit version of the Java SDK from SUN Microsystems (Oracle).

For Mac OS X systems: the Java 64-Bit SDK from Apple Inc. is also supported by Proxy Sniffer but this requires that at least OS X Version 10.6 (Snow Leopard) is installed.

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 data transfer 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. Furthermore, 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 Proxy Sniffer, even if your machine runs with Windows 64-Bit.

Note: Different operating systems can be mixed. For example, the Proxy Sniffer GUI can be installed on a Windows System and the Load Generators (Exec Agents) can be installed on Unix-like Systems.
1.3 Installation on Windows

Start **Prx52<minor version>-exe** and follow the installation instructions. If you accept the suggested settings you don't require administrator rights. In combination with installing the Firefox Portable web browser (see next chapter 1.3.1) no administrator rights are required to use all functionality of the Proxy Sniffer product.

During the installation you must enter (or review) your license data. After that click on the Apply button:

Note: if you install only the GUI component of Proxy Sniffer, 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 Proxy Sniffer installation directory.

After installation, 3 new icons are placed on the desktop, and new entries are created in the **Start ▶ All Programs ▶ ProxySniffer** menu.

If you wish, you can delete the 3 desktop icons – the same icons can also be called from the start menu.

**Start Proxy Sniffer** by first clicking on the **Proxy Sniffer Console** icon, and then by clicking on the **Proxy Sniffer GUI** icon.
In Start ➤ All Programs ➤ ProxySniffer you will find also A Guide to Getting Started with Successful Load Testing, and the Application Reference Manual which describes the Proxy Sniffer system architecture and all programs and utilities which are delivered with the product.
1.3.1 Further Hints for using Proxy Sniffer on Windows - Firefox Portable and Firefox Recording Extension

Accessing the Proxy Sniffer GUI and recording of Web surfing sessions is fully supported by using the Microsoft Internet Explorer (see chapter 3.3.1). 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](http://portableapps.com/apps/internet/firefox_portable) and install it inside your \Users directory:

After that you should download the **Firefox Recording Extension** from [https://www.proxy-sniffer.com/download/PrxRecExt1.xpi](https://www.proxy-sniffer.com/download/PrxRecExt1.xpi).

Then start the **Firefox Portable** Web Browser and install the **Firefox Recording Extension**:

Click on the [i] icon and follow the instructions to configure the recommended Firefox options.

**Note:** using the Firefox Recording Extension requires that the Proxy Sniffer 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 “Proxy Sniffer Toolbar” in the web browser menu “View” ➔ “Toolbars”.


FAQ:

Q: After updating Firefox a newer version the "Firefox Recording Extension" does not longer work.

A: there is always a new version of the "Firefox Recording Extension" available which supports the latest Firefox version (compatible with all Firefox versions starting from version 3.0). Upgrade instructions: first uninstall the "Firefox Recording Extension" inside your Web browser. After that download and install the new version from https://www.proxy-sniffer.com/download/PrxRecExt1.xpi
1.3.2 Windows System Tuning

It is strongly recommended that you tune the operating system on which Proxy Sniffer is installed, especially if the error "Network Error at Client Side" occurs during a load test, or if some real-time statistic data are not shown in the Web Admin GUI during a load test (appearing as broken images in the Web browser).

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 web 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.
1.3.2.2  Windows XP
Increase the number of free TCP/IP client sockets by adding the following new entries with regedit. Afterwards you must reboot the system in order for the changes to take effect.

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value (decimal)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxFreeTcbs</td>
<td>20000</td>
<td>(REG_DWORD, decimal)</td>
</tr>
<tr>
<td>TcpTimedWaitDelay</td>
<td>30</td>
<td>(REG_DWORD, decimal)</td>
</tr>
</tbody>
</table>

1.3.2.3  Windows 2003 Server
Increase the number of free TCP/IP client sockets by adding the following new entries with regedit. Afterwards you must reboot the system in order for the changes to take effect.

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value (decimal)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SynAttackProtect</td>
<td>0</td>
<td>(REG_DWORD, decimal)</td>
</tr>
<tr>
<td>TcpTimedWaitDelay</td>
<td>30</td>
<td>(REG_DWORD, decimal)</td>
</tr>
<tr>
<td>MaxFreeTcbs</td>
<td>20000</td>
<td>(REG_DWORD, decimal)</td>
</tr>
<tr>
<td>MaxUserPort</td>
<td>65534</td>
<td>(REG_DWORD, decimal)</td>
</tr>
<tr>
<td>MaxUserPorts</td>
<td>65534</td>
<td>(REG_DWORD, decimal)</td>
</tr>
</tbody>
</table>

1.3.2.4  Windows 7 and Windows 2008 Server
Increase the number of free TCP/IP client sockets by performing the following two actions:

   a) Enter the following command from a command terminal:
      `netsh int ipv4 set dynamicport tcp start=12288 num=53247`

   b) Add the following new entry with regedit.
      \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value (decimal)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>TcpTimedWaitDelay</td>
<td>30</td>
<td>(REG_DWORD, decimal)</td>
</tr>
</tbody>
</table>

Afterwards you must reboot the system in order for the changes to take effect.
1.4 Installation on Mac OS X

Expand the archive Prx52<minor version>.zip with one mouse click and then start the installation by clicking on Prx52<minor version>.app. Follow the installation instructions. We recommend to install Proxy Sniffer into the proposed folder /Applications if you have administrator rights. If you do not have administrator rights, you should install Proxy Sniffer inside your home folder /Users/<your account name>. After installation, 3 new icons are placed on the desktop, and new entries are created in the Applications ➤ ProxySniffer folder or in the <your account name> ➤ ProxySniffer folder. If you wish, you can delete the 3 desktop icons.

Start Proxy Sniffer by first clicking on the Proxy Sniffer Console icon, and then by clicking on the Proxy Sniffer GUI icon – or by first clicking on Proxy Sniffer Console.app, and then by clicking on ProxySnifferGUI.html. Alternatively you can also access the GUI by starting the Firefox Web Browser and entering http://127.0.0.1:7990 into the web browser. The Firefox Recording Extension is also supported on Mac OS X systems (see chapter 3).

Notes: you will find the full Proxy Sniffer documentation in the installation directory, inside the subdirectory doc. The installation kit installs also an uninstaller-script which is located the "Uninstall Apica ProxySniffer" folder.
1.4.1 Mac OS X System Tuning

The default OS-settings for the maximum number of network connections per process is restricted 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 value is too small to execute load tests from Mac OS X and it is also too small to monitor remotely executed cluster jobs. Therefore we strongly recommend that you tune your Mac OS X system and increase this value at least to 12288.

Tuning instructions:

1. Get first the system-wide configuration for the maximum number of network connections by entering "sysctl kern.maxfiles" from a terminal. Typically you will see a value of 12288.

2. Edit or create the file /etc/launchd.conf by entering "sudo vi /etc/launchd.conf" from a terminal. On most Mac OS X systems this file does not yet exist.

3. Add the following line to launchd.conf:

```plaintext
limit maxfiles 12288 12288
```

Note: instead of 12288 you should use the actual value of sysctl kern.maxfiles, and please do not configure "unlimited" for this value.

4. You may also add the following line to increase the number of threads that can be used per process:

```plaintext
limit maxproc 2048 2048
```

5. Enter "exit" in your terminal and reboot your system.

6. After rebooting, enter once again "ulimit -n" in a terminal. You should now see a value of 12288.
1.4.2 Mac OS X Java Modification / Edit java.security

All of the Java implementations on Mac OS X systems do not load Java "Security Providers" in a dynamic way. Therefore you have to add manually a new Java security provider called "iaik.security.provider.IAIK" which is required for ProxySniffer. If you miss this post-installation step ProxySniffer 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
   ```

Note: If you find several files of java.security on your machine we recommend that you edit all of them.
1.4.3 Special Instructions for Mac OS X 10.9 (or newer) / Prevent "App Nap"

After installing ProxySniffer you have to disable (prevent) "App Nap" for the "Proxy Sniffer Console". Use Finder and navigate to the ProxySniffer installation directory (typically located at /Applications/ProxySniffer). Then click at the file "Proxy Sniffer Console" and choose Finder ► File ► Get Info.

After that Prevent App Nap by selecting the corresponding checkbox.
1.4.4 Special Instructions for Java 7 on Mac OS X 10.8 (or newer)

If you have already installed Java 7 on your Mac OS X 10.8 system it might be the case that you cannot run any compiled load test program because the "Execute Load Test" icons are not shown in the "Project Navigator" menu.

The problem with Java 1.7 on Mac OS X 10.8.2 is that the Proxy Sniffer console still runs under Java 1.6, even when Java 1.7 was installed. This effects, that the Load Test programs are compiled with Java 1.7 (because the compiler is started as a process), but then should be loaded and executed by Java 1.6 - which does not work.

Therefore, you have to configure Proxy Sniffer in such a way that Java 1.6 is used to compile the load test programs. First, all Java SDK should be searched on the system by entering:

```
sudo find / -name javac -print
```

```
find: /dev/fd/3: Not a directory
find: /dev/fd/4: Not a directory
/Library/Java/JavaVirtualMachines/jdk1.7.0_09.jdk/Contents/Home/bin/javac
/System/Library/Frameworks/JavaVM.framework/Versions/A/Commands/javac
/System/Library/Java/JavaVirtualMachines/1.6.0.jdk/Contents/Commands/javac
/System/Library/Java/JavaVirtualMachines/1.6.0.jdk/Contents/Home/bin/javac
/usr/bin/javac
```
in this case
/System/Library/Java/JavaVirtualMachines/1.6.0.jdk/Contents/Home/bin/javac
is used by the Proxy Sniffer console.

Now, Proxy Sniffer can be configured to use the Java 1.6 compiler:

Project Navigator -> Setup (gearwheel icon), set:
Java Compiler Invocation (Path) = /System/Library/Java/JavaVirtualMachines/1.6.0.jdk/Contents/Home/bin/javac
Java Interpreter Invocation (Path) = /System/Library/Java/JavaVirtualMachines/1.6.0.jdk/Contents/Home/bin/java (without a 'c' at the end)

Now, the Proxy Sniffer console should be restarted and the load test programs (*.java) must be compiled again using Project navigator. After that it will work.
Additionally, you have to **configure the IAIK security** provider as described in chapter 1.4.2.

**sudo find / -name "java.security" -print**
Applications/Xcode.app/Contents/Applications/Application Loader.app/Contents/MacOS/itunes/java/lib/security/java.security
find: /dev/fd/3: Not a directory
find: /dev/fd/4: Not a directory
/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security/java.security
/Library/Java/JavaVirtualMachines/jdk1.7.0_09.jdk/Contents/Home/jre/lib/security/java.security
/System/Library/Java/JavaVirtualMachines/1.6.0.jdk/Contents/Home/lib/security/java.security

**In this example, the following two files should be updated:**
/Library/Java/JavaVirtualMachines/jdk1.7.0_09.jdk/Contents/Home/jre/lib/security/java.security (and)
/System/Library/Java/JavaVirtualMachines/1.6.0.jdk/Contents/Home/lib/security/java.security

Finally you should also tune the OS by creating the file `/etc/launchd.conf` with the following content (after that reboot the OS)

```bash
limit maxfiles 12288 12288
limit maxproc 2048 2048
```
1.5 Installation on Ubuntu (Linux)

The standard Ubuntu distribution contains normally no preinstalled JDK (Java Development Kit) from SUN (Oracle). Therefore you have first to install the original JDK from SUN Microsystems.

Proceed as follows to install the Java SDK on Ubuntu:

- Open a terminal and enter:

  `sudo apt-get install sun-java6-bin sun-java6-jre sun-java6-jdk`

- During the installation you are asked to accept the license conditions of SUN Microsystems. Press the <TAB> key until the <Ok> input field is highlighted in red color and then press <Return>. After that you’ll be prompted again, where you have to agree to the “license terms” by selecting <Yes>.

- After the installation has completed enter “java -version” inside the terminal to check that the right Java distribution from SUN is used:

  ![Java Version Command](image)

- For further help you may have a look on the following two web sites:
  

Now you can install Proxy Sniffer on Ubuntu:

Download Prx50<minor version>.bin and save it on your Desktop.

1. Open a terminal and enter:

   `cd Desktop`

2. After that start the installation by entering:

   `sh ./Prx50<minor version>.bin`
3. Follow the instructions. Normally you should install Proxy Sniffer in the suggested directory.

![Choose Install Folder](image1)

4. During the installation you must enter (or review) your license data. After that **click on the Apply button:**

![Proxy Sniffer Settings and License](image2)
5. After that the installation is completed

You can now **start Proxy Sniffer** by first clicking on the Proxy Sniffer Console icon …
... and then start the Firefox Web Browser and enter http://127.0.0.1:7990

We recommend that you also install the Firefox Recording Extension (a Firefox Add-On) – see chapter 3 in this document.
Note: you will find the full Proxy Sniffer documentation in the installation directory, inside the subdirectory doc:

The installation kit installs also an uninstaller:
1.6 Installation on all other Unix-like Systems (Linux, Solaris, BSD …)

1. Manually create the installation directory /usr/local/prxsniff (you may choose also any other installation directory)

2. Copy the files prxsniff.jar, iaik_jce_full.jar, iaik_ssl.jar, iaik_eccelerate.jar, iaikPkcs11Provider.jar, root.cer and privkey.der to this directory (you can copy this files from a Windows or a Mac OS X or, from an Ubuntu installation of Proxy Sniffer. These files can be used for all operating systems).

3. Create the files prxsniff.key and ExecAgentTicket.dat inside the installation directory by using vi or another text editor. These files must contain (as ASCII text) the Proxy Sniffer 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 the files prxsniff.jar, iaik_jce_full.jar, iaik_ssl.jar, iaik_eccelerate.jar and iaikPkcs11Provider.jar


5. Start Proxy Sniffer with the following command:

```
java -Xmx1024m ProxySniffer -WebAdmin -JobController -ExecAgent -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 also supported on all Unix-like systems.

Alternatively to the steps 4 and 5 above you can start on Unix-like systems Proxy Sniffer in “GUI console mode” by using the following commands:

```
cd /usr/local/prxsniff
export CLASSPATH=.:prxsniff.jar:
iain_jce_full.jar:iaik_ssl.jar:iaik_eccelerate.jar:iaikPkcs11Provider.jar
java -Xmx1024m ProxySnifferConsole -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.

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 option

**Note for starting an Exec Agent as an Independent Process** (Load Generator, without Proxy Sniffer GUI):
Use the following command:
```
nohup java -Xmx768m -server ExecAgent -tz ECT 2>&1 > ExecAgent.log &
```

You may also add the option -jobdir and -dgs. Please take a look at chapter 3.3 of the Application Reference Manual.
1.6.1 Unix-Like System Tuning (Solaris, Linux, BSD …)

By Using “ulimit -n <max value>”, increase the maximum number of open files, and open network connections, allowed for each process. Entering “ulimit -n” without a number displays the current value. Recommended value: 32768 or higher.

For Linux systems we recommend also that you increase the IP port range by entering the following command from a terminal:

```bash
echo "net.ipv4.ip_local_port_range = 1024 65535" >> /etc/sysctl.conf
```

1.7 Post Installation / Security Hint for all Operating Systems

The "Proxy Recorder" of Proxy Sniffer 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 Proxy Sniffer installation kit and could be directly imported in any operating system and in any Web Browser product in order to prevent Web Browser warnings about an unknown CA root. But consider that all other customers are also able to generated faked HTTPS Web server certificates by using the same CA root certificate of the installation kit !!! Therefore, if you import the file "root.cer" delivered by the Proxy Sniffer installation kit the security of your operating system and Web Browser will be severe damaged (file "root.cer" located in the Proxy Sniffer installation directory). You would trust to any Web server certificate issued by any other customer of Proxy Sniffer.

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

Instead of that we strongly recommend that you create our own (private) CA root certificate by using the OpenSSL toolkit (OpenSSL is not part of the Proxy Sniffer installation kit). You can use any Unix-like system to generate your own CA root certificate. Proceed as follows:

1. openssl req -newkey rsa:2048 -days 7305 -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)

After that you have to replace in the Proxy Sniffer installation directory the two files "root.cer" and "privkey.der" with your own versions. Finally you must restart Proxy Sniffer (stop and start the console). Note: the CA root certificate is not used on the Load Generators (GUI only).

Now you can also import our own (private) CA root certificate into the operating system and in 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 certificate with anybody else.

See also: Appendix A: How to create your own CA Root Certificate on Windows Systems
2 Architecture Overview

2.1.1 Local Architecture

The Proxy Sniffer Console contains four built-in servers which are started on your local computer:

1. **Proxy Sniffer**: A special proxy server which is used to record web surfing sessions.
2. **Web Admin**: An embedded, local web server for the web GUI.
3. **Exec Agent**: A server which allows the execution of load tests as “batch jobs”.
4. **Job Controller**: A server which allows to combine several load-releasing systems into an Exec Agent cluster.

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

<table>
<thead>
<tr>
<th>TCP/IP Port Number</th>
<th>Port Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7990</td>
<td>Embedded web server, GUI (Web Admin)</td>
</tr>
<tr>
<td>7993</td>
<td>Load Test executing server (Exec Agent)</td>
</tr>
<tr>
<td>7995</td>
<td>Support for Exec Agent clusters (Job Controller)</td>
</tr>
<tr>
<td>7997</td>
<td>Internal communication port (Proxy Sniffer Server)</td>
</tr>
<tr>
<td>7998</td>
<td>HTTP proxy port (Proxy Sniffer Server)</td>
</tr>
<tr>
<td>7999</td>
<td>HTTPS proxy port (Proxy Sniffer Server)</td>
</tr>
</tbody>
</table>
- Web Browser
- Web Service Client Application
- Web Client Tool (e.g. curl)
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 Proxy Sniffer 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 Proxy Sniffer 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:

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 (see www.gcloud.com), or can be accessed by purchasing an "Unlimited Exec Agent Short-Time License" (see www.proxy-sniffer.com/ec2.html)

Several Exec Agents can also 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 computers of a load-generating cluster (the cluster members) may 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 the 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 HTTP/S proxy server means, in this case, that load tests can be started from a protected corporate network and then transmitted, over the proxy server of the corporation, to any load releasing system 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).
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://<proxy-sniffer-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 the 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

Perform the following steps to enable the remote access protection for the Web Admin GUI:

1. Open a command terminal and navigate into the Proxy Sniffer installation directory.
2. Set the Java CLASSPATH:
   - On Windows systems enter: `set CLASSPATH=.;prxsniff.jar;iaik_jce_full.jar;iaik_ssl.jar;iaik_eccelerate.jar;iaikPkcs11Provider.jar`
3. Create a super user account by calling the Proxy Sniffer account utility as follows:
   `java WebAdminLoginAccounts`
   You will see the following menu:

<table>
<thead>
<tr>
<th>Select</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>list all accounts</td>
</tr>
<tr>
<td>2</td>
<td>reset password</td>
</tr>
<tr>
<td>3</td>
<td>enable account</td>
</tr>
<tr>
<td>4</td>
<td>disable account</td>
</tr>
<tr>
<td>5</td>
<td>set superuser</td>
</tr>
<tr>
<td>6</td>
<td>remove superuser</td>
</tr>
<tr>
<td>7</td>
<td>add account</td>
</tr>
<tr>
<td>8</td>
<td>delete account</td>
</tr>
<tr>
<td>9</td>
<td>delete file WebAdminLoginAccounts.dat - disable any protection and delete all accounts</td>
</tr>
<tr>
<td>0</td>
<td>exit</td>
</tr>
</tbody>
</table>

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

4. Optional Step: 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:

![Remote Access Protection Activated](image)

5. On any other system, start a Web browser and enter http://<proxy-sniffer-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:
6. 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:
7. **Note**: if a logged in user *does not have super user privileges* the functionality of this menu is limited, and allows only to change the own password.
3 Reconfiguring the Web Browser for Recording of Web Surfing Sessions

Note: if you are planning to use a Firefox Web Browser for the recording of Web surfing sessions, you can skip this chapter. Instead of this it is recommended that you download and install the Firefox Recording Extension from https://www.proxy-sniffer.com/download/PrxRecExt1.xpi

After installation click on the icon inside the Firefox Recording Extension and follow the instructions:

Recording of web surfing sessions is supported by using any Web browser, such as Internet Explorer or Safari. You can also use Firefox without installing the Firefox Recording Extension.

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

Before using Proxy Sniffer, 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**. Please 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 configuration dialog directly from the Internet Options 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:

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

### 3.2 JavaScript Settings for Firefox

If you use Mozilla Firefox you must also configure the "Advanced JavaScript Settings".

Please enable the following checkboxes:

- Move or resize existing windows
- **Raise or lower windows**
- Disable or replace context menus
3.3 Reconfiguring a Web Browser for Recording

You must now reconfigure a web browser to use Proxy Sniffer for recording web surfing sessions. This means that the web browser must be reconfigured in such a way, that the data traffic flows over the local **Proxy 127.0.0.1** by using the TCP/IP port **7999** for unencrypted **HTTP** connections and by using the TCP/IP port **7997** for encrypted **HTTPS** connections.

You may use the same web browser product for recording load tests and for using the Web Admin GUI, or you may 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 Proxy Sniffer. Note also that the proxy configuration of the web browser is not needed during the execution of load tests.

---

**Hint:** Cascading Proxy Sniffer with an outbound proxy server of your company is also supported as an optional configuration. Use this option if you only have an indirect network connection from your local workstation (located inside a protected corporate network), over an outbound proxy server, to the external target web server. The outbound proxy server can be configured in the Personal Settings menu which is accessible from the main menu.
3.3.1 Microsoft Internet Explorer Proxy Configuration

If your IT department has disabled the "Connections" menu inside the IE internet options, you may try to re-enable it by using `regedit`. Set "HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel\ConnectionsTab" from 1 to the value of 0 (0=enabled).
3.3.2 Firefox Proxy Configuration

3.3.3 Safari Proxy Configuration
3.3.4 Web Browser Warning Messages (HTTPS)

If you record encrypted HTTPS data with Proxy Sniffer, the web browser will display a security alert. This is “normal” behavior when - and only when - using Proxy Sniffer because the integrated SSL tunnel will decrypt the data (for recording), and will generate on-the-fly a faked and invalid server certificate. The format of this warning message depends on the web browser you are using. To continue recording, you must click one or more times through to the “continue” or “ignore” button.

Important Hint: Never ignore these kinds of error messages when not recording web sessions with Proxy Sniffer; that is, during normal web surfing. The apparent secure connection to the web server may actually be insecure, and might be wiretapped or modified by cyber-criminals in this situation.

Microsoft Internet Explorer 7

Firefox 2

Safari

Firefox 3 – Step 1/2

Firefox 3 – Step 2/2
3.4 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.

Internet Explorer

Firefox

Safari
4 Next Steps for Recording Web Surfing Sessions and Executing Load Tests

Please take some time to read the Proxy Sniffer User's Guide (PDF). You will learn many things about using advanced Proxy Sniffer features.
Appendix A: How to create your own CA Root Certificate on Windows Systems

   We recommend that you select "Win32 OpenSSL v1.0.1c" (or a newer version). During installation ignore any warnings of OpenSSL.

   Alternatively, you can download OpenSSL for Windows also from our Web site: http://www.proxy-sniffer.com/download/Win32OpenSSL-1_0_1c.exe

   Note: in the following steps OpenSSL was installed in the folder
   C:\OpenSSL-Win32

2. Download the file openssl-prx.cfg from http://www.proxy-sniffer.com/download/openssl-prx.cfg and store it in the .\bin directory of OpenSSL
   (in this example: C:\OpenSSL-Win32\bin\openssl-prx.cfg)

3. Open a Command Prompt terminal (run → cmd.exe) and set the environment variable OPENSSL_CONF to the absolute file path of openssl-prx.cfg. Example:

   SET OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl-prx.cfg

4. In the Command Prompt terminal navigate to any directory and create your CA Root certificate by entering the following command:

   C:\OpenSSL-Win32\bin\openssl req -newkey rsa:2048 -days 7305 -x509 -extensions v3_ca -nodes -out root.cer

   Example:
   C:\Scratch> C:\OpenSSL-Win32\bin\openssl req -newkey rsa:2048 -days 7305 -x509 -extensions v3_ca -nodes -out root.cer
   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 LLC
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) []: Own Created Proxy Sniffer Root Certificate

C:\Scratch>

The two files root.cer and privkey.pem are now created.

5. Convert the private key by entering the following command:

   C:\OpenSSL-Win32\bin\openssl pkcs8 -topk8 -nocrypt -in privkey.pem -outform der -out privkey.der

   The file privkey.der is now created.

6. Copy the files root.cer and privkey.der into the Proxy Sniffer installation directory. Example:

   C:\Scratch>copy /y root.cer C:\Users\mutong\ProxySniffer
   1 file(s) copied.

   C:\Scratch>copy /y privkey.der C:\Users\mutong\ProxySniffer
   1 file(s) copied.

   Note: the old existing files must be replaced / overwritten.

7. Delete inside the Proxy Sniffer installation directory all files with the file extension *.crt and *.privkey. These files are old HTTPS Web server certificates generated by the (old) common CA root certificate. If you have never recorded before an encrypted HTTPS session no such files exists. Typical names of such files that you have to delete are for example:

   sb-ssl_google_com.crt
   sb-ssl_google_com.privkey
8. Start the Proxy Sniffer Console and the Proxy Sniffer GUI and then click on the CA root certificate icon:

You should see now your own created CA root certificate:
9. Restart the Proxy Sniffer Console once again (stop and start the Proxy Sniffer Console).

10. You can now import your CA root certificate into Firefox and into the Windows operating system, and also into an iOS device such as an iPhone or an iPad.

Import your CA root certificate into Firefox:
Select File containing CA certificate(s) to import

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "Own Created Proxy Sniffer Root Certificate" for the following purposes?

- ✔ Trust this CA to identify websites.
- ✔ Trust this CA to identify email users.
- ✔ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View
Examine CA certificate

OK
Cancel
### Certificate Manager

You have certificates on file that identify these certificate authorities:

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Security Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Secure Server Authority</td>
<td>Software Security Device</td>
</tr>
<tr>
<td>OpenSSL</td>
<td>Software Security Device</td>
</tr>
<tr>
<td>My Company LLC</td>
<td>Software Security Device</td>
</tr>
<tr>
<td>Own Created Proxy Sniffer Root Certificate</td>
<td>Software Security Device</td>
</tr>
<tr>
<td>NetLock Minisite Kozjevnik (Class C) TANUSYSTEMKADO</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>NetLock Kozjevnik (Class A) TANUSYSTEMKADO</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>NetLock Windows (Class B) TANUSYSTEMKADO</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>Netlock Express (Class C) TANUSYSTEMKADO</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>NOTLock rtf</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>NetLock Army (Class G) FSTABALABY</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>Network Solutions LLC.C</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>Network Solutions Certificate Authority</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>PM/JOCON</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>IGCA</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>QuoVads Limited</td>
<td>Built-in Object Token</td>
</tr>
<tr>
<td>Coop Root CA 1</td>
<td>Software Security Device</td>
</tr>
</tbody>
</table>
Import your CA root certificate into the Windows operating system:
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

- **Issued to:** Own Created Proxy Sniffer Root Certificate
- **Issued by:** Own Created Proxy Sniffer Root Certificate
- **Valid from:** 18. 06. 2012 to 19. 06. 2022
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a verification of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.
The Certificate Import Wizard window is shown.

- **Certificate Store**: Certificate stores are system areas where certificates are kept.
  - Windows can automatically select a certificate store, or you can specify a location for the certificate.
  - For custom store selection:
    - **Automatically select the certificate store based on the type of certificate**
    - **Browse all certificates in the following store**

- **Select Certificate Store**: Select the certificate store you want to use.
  - **Personal**: Trusted Root Certification Authorities, Enterprise Trust, Intermediate Certification Authorities, Trusted Publishers, Untrusted Certificates
  - **Show physical stores**
Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

- Automatically select the certificate store based on the type of certificate
- Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities

Learn more about certificate stores

< Back  Next >  Cancel
You are about to install a certificate from a certification authority (CA) claiming to represent:

Own Created Proxy Sniffer Root Certificate

Windows cannot validate that the certificate is actually from "Own Created Proxy Sniffer Root Certificate". You should confirm its origin by contacting "Own Created Proxy Sniffer Root Certificate". The following number will assist you in this process:


Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes
No

The import was successful.
Appendix B: 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 it's 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:
Unverified Profile

The authenticity of "Own Created Proxy Sniffer Root Certificate" cannot be verified. Installing this profile will change settings on your iPad.

Root Certificate

Installing the certificate "Own Created Proxy Sniffer Root Certificate" will add it to the list of trusted certificates on your iPad.
Enter your iPad password – if your iPad is protected by a password. Do **not** enter your Apple ID password.