

Installing the GTA SSL Sentinel Client

SSLLinux201003-01



Global Technology Associates
3505 Lake Lynda Drive Suite 109
Orlando, FL 32817

Tel: +1.407.380.0220
Fax: +1.407.380.6080
Email: info@gta.com
Web: www.gta.com

Installing the SSL Sentinel Client: Linux

This section will assist users in the download, installation, and configuration of the SSL Sentinel Client.

Requirements

- GB-OS 5.3.0 or higher
- Linux system with Tun/Tap support enabled in kernel (available with Linux 2.4 and higher)
- Root access on the Linux system
- SSL Sentinel Client
- User access permissions for the SSL Sentinel Browser and Client on the firewall
- The host name or an IP Address assigned to the firewall's External Interface
- Downloaded client and configuration files. All required files may be downloaded via the firewall Web interface.

Accessing the GTA Remote Access Portal for Download

To access the GTA Remote Access Portal, open a Web browser and enter the IP address or host name of your firewall. If the firewall's SSL Sentinel Browser is configured for a port other than 443, append with a colon and port number.

Example: <https://ssl.gta.com:1443>



Figure 1: Location Bar with Non Standard Port

The login screen for the GTA Remote Access Portal will display. Enter your user login credentials to access the browser. If the virtual keyboard is required, you will have to use the virtual keyboard to enter your password. Use the shift key to access special characters.

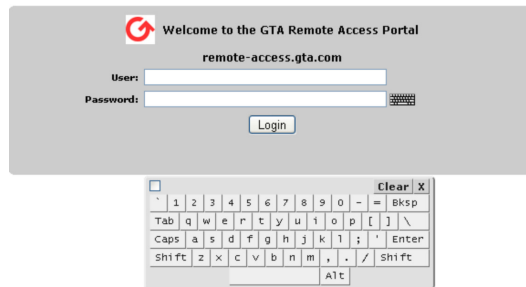


Figure 2: Remote Access Login



Note

Administrators with SSL privileges logging in on the administration port will see the normal firewall administration interface and the SSL Sentinel Browser.

Download the SSL Sentinel Certificates and Configuration Files

All needed files can be downloaded from the Web interface at **SSL Sentinel>Client**.

1. Click on the **LINUX/UNIX – CLIENT CONFIGURATION BUNDLE DOWNLOAD**.
 - a. The users client configuration file and certificates will be downloaded in a zip file (including the CA certificate).
 - b. The configuration file should be downloaded to your home directory (example: /home/user or /home/user/Download).

Linux / Unix	
Linux / Unix Source	Requires manual installation. Download
Client Configuration Bundle	Zip file containing a customized client configuration, and the required certificates to establish an SSL Sentinel Client connection. Download
Installation Guide	The installation guide contains instructions on how to install the Linux / Unix version of the SSL Sentinel Client. Download

Figure 3: Linux/Unix Install Files



2. Unzip the Client Configuration Bundle.

```
> unzip client.zip
```

**Note**

This will create a folder with the firewall's host name.

3. For systems running selinux in enforcing mode, please perform the following steps:
 - a. Enable OpenVPN Home Directory Permissions.

```
> setsebool -P openvpn_enable_homedirs 1
```

**Note**

To temporarily (change will no longer be present after system reboot) set the selinux Boolean do not use the '-P' option.

- b. Restore Conetext of all of the Certificates and Key files that will be used.

```
> restorecon -v /home/user/Download/firewall.example/user.crt
> restorecon -v /home/user/Download/firewall.example/user.key
> restorecon -v /home/user/Download/firewall.example/ca.crt
```

Install OpenVPN

1. Using package manager (requires root privileges).
 - a. Ubuntu/Debian

```
> apt-get openvpn
```
 - b. Fedora/Red Hat

```
> yum install openvpn
```
2. Source code from the firewall (requires c++ compiler).
 - a. Login to SSL Sentinel Interface.
 - b. Navigate to **SSL Sentinel>Client**.
 - c. Click on Linux / Unix Source download. This will download the source code.
 - d. Extract the source code.

```
> tar -xzf openvpn.tar.gz
```
 - f. Change directories to the top-level of the extracted folder.
 - g. Make and Install the Package.

```
> ./configure
> make
> make install
```
3. Download and Install from OpenVPN.
 - a. Download - <http://www.openvpn.net/index.php/open-source/downloads.html>
 - b. Install Instructions - <http://www.openvpn.net/index.php/open-source/documentation/howto.html#install>

Opening the Tunnel Using Command Line

1. Open a terminal.
2. Change directory to the location the downloaded zip file was extracted.
> `cd /home/user/Download/`
3. Execute Open VPN with the Configuration File (requires root privilege).
> `openvpn --config firewall.example.ovpn`
4. Enter User Credentials (open VPN will prompt your SSL Sentinel User Credentials).
> Enter Auth Username: `user`
> Enter Auth Password:

Install Network Manager Plug-In

Not required if using OpenVPN command line.

1. Using package manager.
 - a. Ubuntu/Debian
> `apt-get NetworkManager-openvpn`
 - b. Fedora/Red Hat
> `yum install NetworkManager-openvpn`

Configure OpenVPN using Network Manager

1. Right click on the **NETWORK MANAGER** icon.
2. Select **EDIT CONNECTIONS**.

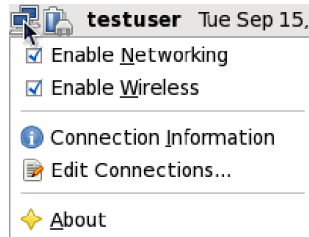


Figure 4: Network Manager Options

3. Select the **VPN** tab and click **ADD**.

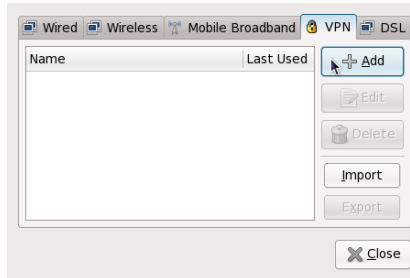


Figure 5: VPN Tab

4. Select the connection type **OPENVPN** and click **CREATE...**



Figure 6: Select Connection Type

5. Enter a CONNECTION NAME.
6. Enter GATEWAY. This will be the IP address of the firewall that you are connecting.

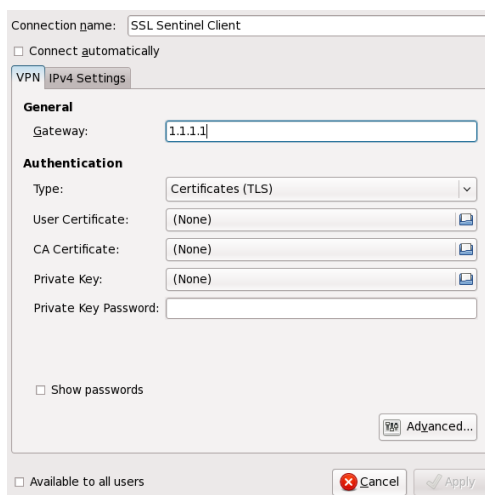


Figure 7: Connection Name and Gateway

7. Select TYPE: PASSWORD WITH CERTIFICATES (TLS).
8. Enter the USERNAME AND PASSWORD configured for your user on the firewall.
9. Select the USER CERTIFICATE. This is the user certificate included in the install bundle.
10. Select the CA CERTIFICATE. This is the firewall's CA certificate included in the install bundle.
11. Select the USER KEY. This is the private key associated with the User Certificate included in the install bundle.



Figure 8: Configure the Connection

12. Click **ADVANCED...**
13. Select the **GENERAL** tab.
14. Enable **USE LZO DATA COMPRESSION** and **USE A TCP CONNECTION**.

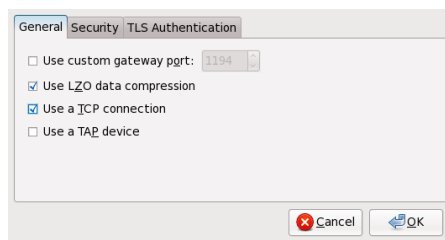


Figure 9: General Tab

15. Select the **SECURITY** tab.
16. Select AES-192-CBC from the CIPHER drop down.
17. Select SHA-1 from the HMAC AUTHENTICATION drop down. The Default is SHA-1.

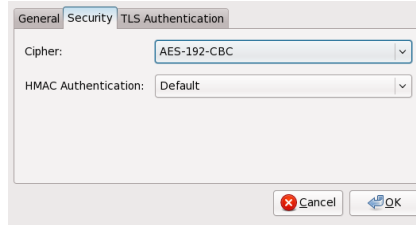


Figure 10: Security

18. Click **OK**.
19. Select the **IPV4 SETTINGS** tab.

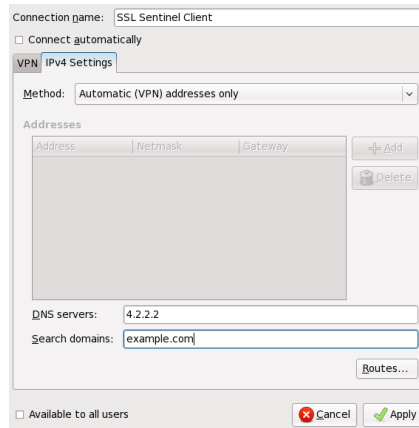


Figure 11: IPV4 Settings

20. Click on **ROUTES**.
21. Check the option **USE THIS CONNECTION ONLY FOR RESOURCES ON ITS NETWORK** (without this option the routes will be such that all traffic will be forced through the OpenVPN client).

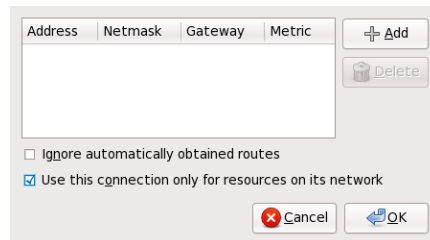


Figure 12: Routes

22. Click **OK**.
23. Click **APPLY**.

Open the Tunnel using Network Manager

1. Left click on the **NETWORK MANAGER** icon.
2. Go to **VPN CONNECTIONS** and select the name of the tunnel you just created.

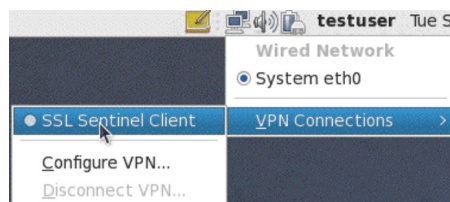


Figure 13: Opening the Tunnel



Copyright

© 1996-2010, Global Technology Associates, Incorporated (GTA). All rights reserved.

Except as permitted under copyright law, no part of this manual may be reproduced or distributed in any form or by any means without the prior permission of Global Technology Associates, Incorporated.

Technical Support

GTA includes 30 days “up and running” installation support from the date of purchase. See GTA's Web site for more information. GTA's direct customers in the USA should call or email GTA using the telephone and email address below. International customers should contact a local Authorized GTA Channel Partner.

Tel: +1.407.380.0220 Email: support@gta.com

Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

Trademarks & Copyrights

GB-OS, Surf Sentinel, Mail Sentinel and GB-Ware are registered trademarks of Global Technology Associates, Incorporated. GB Commander is a trademark of Global Technology Associates, Incorporated. Global Technology Associates and GTA are service marks of Global Technology Associates, Incorporated.

Microsoft, Internet Explorer, Microsoft SQL and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe and Adobe Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

UNIX is a registered trademark of The Open Group.

Linux is a registered trademark of Linus Torvalds.

BIND is a trademark of the Internet Systems Consortium, Incorporated and University of California, Berkeley.

WELF and WebTrends are trademarks of NetIQ.

Sun, Sun Microsystems, Solaris and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Java software may include software licensed from RSA Security, Inc.

Some products contain software licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

Some products include software developed by the OpenSSL Project (<http://www.openssl.org/>).

Mailshell and Mailshell Anti-Spam is a trademark of Mailshell Incorporated. Some products contain technology licensed from Mailshell Incorporated.

All other products are trademarks of their respective companies.

Global Technology Associates, Inc.

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA

Tel: +1.407.380.0220 • Fax: +1.407.380.6080 • Web: <http://www.gta.com> • Email: info@gta.com