SOPHOS

simple + secure

# Astaro Security Gateway V7

## Remote Access via IPSec
## Configuring ASG and Client

# 1. Introduction

The guides contain complementary information on the Administration Guide and the Online Help. If you are not sure whether you have the current version of this guide, you can download it from the following Internet address:
http://www.astaro.com/kb

If you have questions or find errors in the guide, please, contact us under the following e-mail address:
documentation@astaro.com

For further help use our support-forum under ...
http://www.astaro.com

... or use the Astaro Support offers ...
http://www.astaro.com/support

# 2. Remote Access via IPSec

This guide describes step by step the configuration of a remote client to access to the Astaro Security Gateway by using IPSec. IPSec allows you, to give individual hosts access to your network through an encrypted IPSec tunnel.

## 2.1. Configuration of the Remote Client

### 2.1.1. Astaro User Portal: Getting Software and Certificates

The **Astaro User Portal** is available for the remote access user. You can use this portal to download guides and tools for the configuration of your client. Especially for the IPSec remote access based on authentication with X.509 certificate, the user portal offers the Astaro Secure Client software (see item 1), the configuration files (see item 2) and necessary keys (see item 3) and configuration guides (see item 4). You should get the following log-in data for the Astaro User Portal from your system administrator: IP address, user name and password.

**1. Start your Browser and open the Astaro User Portal:**

Start your browser and enter the management address of the **Astaro User Portal** as follows: **https://IP address** (example: https://192.168.2.100).

A security notice will appear. Accept the security notice by clicking **OK** (Mozilla Firefox) or **Yes** (Internet Explorer).

**2. Log in to the Astaro UserPortal:**

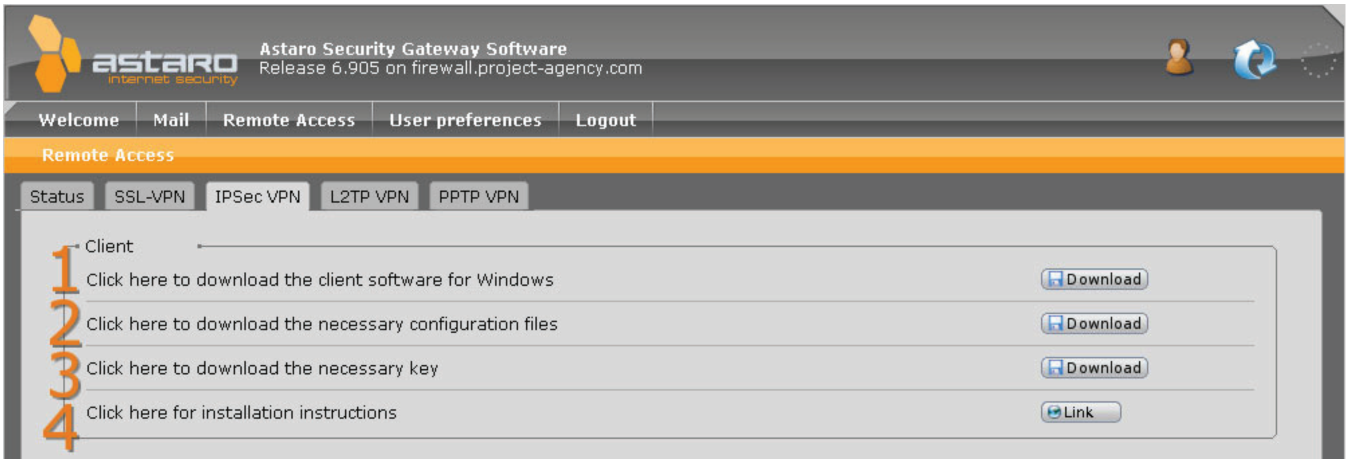
**Username:** Your username, which you received from the administrator.
**Password:** Your password, which you received from the administrator.

Please note that passwords are case-sensitive! Click **Login**.

### 3. Load the tools for the IPSec Remote Access to your client:

The **IPSec VPN** tab will contain the software, configuration files and keys for your client. The Astaro Secure Client runs on Microsoft Windows 98SE, ME, NT 4.0 Service Pack 5 (SP5), 2000 and XP. Start the download process by clicking on **Download**.

Close the Astaro User Portal session by clicking on **Logout**.
The rest of the configuration takes place on the Astaro Security Client.



Click here to download the client software for Windows

Click here to download the necessary configuration files

Click here to download the necessary key

Click here for installation instructions

## 2.1.2. Astaro Secure Client: Configuring the Client

Through the **Profile Import** function (see item 1) the profile settings of the INI file can be automatically imported by the **Astaro Secure Client**. The INI file can either be created by the destination system with an appropriate export function or be edited manually.

In order to set up the Astaro Secure Client, the following steps need to be performed:

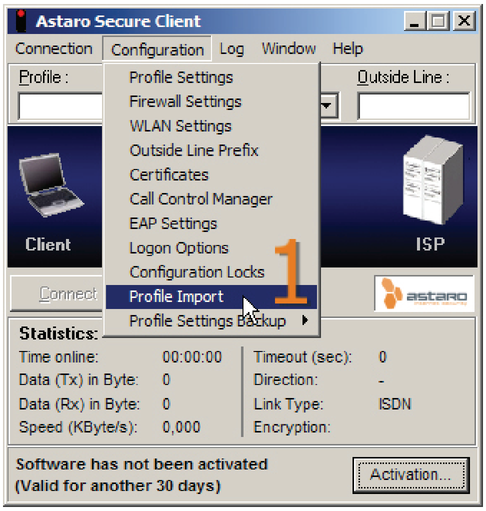
### 1. Import the User's Configuration File.

Start the **Profile Import** wizard by clicking **Configuration** >> **Profile Import**. Store the profile and close afterwards the profile import wizard by clicking **OK**.

### 2. Import the PKCS#12 file.

Open the menu **Configuration** >> **Certificates** on **Astaro Secure Client**. As Certificate, select from **PKCS#12 File**. Then click on the button next to **PKCS#12 Filename**. Browse for the PKCS#12 file of the user and select it.

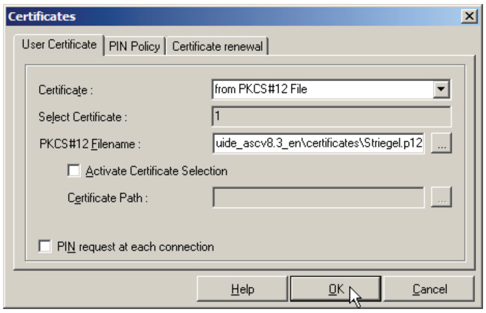
Store the key by clicking **OK**.



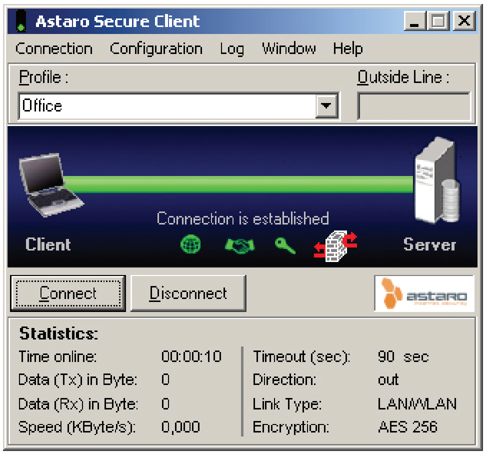
Statistics:

Time online: 00:00:00
Data (Tx) in Byte: 0
Data (Rx) in Byte: 0
Speed (KByte/s): 0,000
Timeout (sec): 0
Direction: -
Link Type: ISDN
Encryption:

Software has not been activated
(Valid for another 30 days)



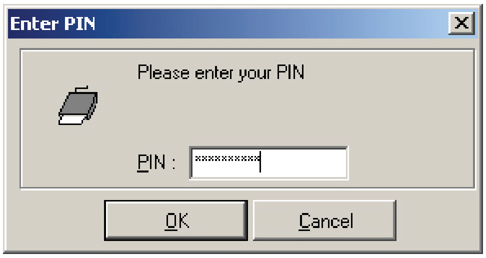
Certificate : from PKCS#12 File
Select Certificate : 1
PKCS#12 Filename : uide_ascv8.3_en\certificates\Striegel.p12
☐ Activate Certificate Selection
Certificate Path :
☐ PIN request at each connection



Profile : Office
Outside Line :
Connection is established

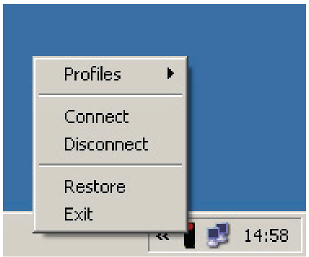
**Statistics:**

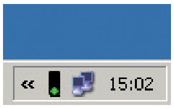
| | | | |
|---|---|---|---|
| Time online: | 00:00:10 | Timeout (sec): | 90 sec |
| Data (Tx) in Byte: | 0 | Direction: | out |
| Data (Rx) in Byte: | 0 | Link Type: | LAN/WLAN |
| Speed (KByte/s): | 0,000 | Encryption: | AES 256 |



Please enter your PIN

PIN : ***********





### 3. Establish a road warrior connection between the client and the destination system.

Click on the **Connect** button.
If the connection establishes successfully, you will see a green bar and the information Connection is established, as can be seen in the screenshot.

If you chose X.509 as authentication method, a **PIN dialog** will show when connecting to the VPN. Enter the **password of the PKCS#12 container** in this case.

**Astaro Secure Client** has a caching mechanism. So during normal operation (connect/disconnect) it is only necessary to enter the PIN once. It is only after a restart of your computer that you need to enter the PIN again.

The client has a **timeout** mechanism included. By default, Astaro Secure Client closes the VPN connection after **100 seconds** of inactivity. In order to increase this value, edit your profile in **Configuration >> Profile Settings** and go to the section **Line Management**. You can specify a higher value in **Inactivity Timeout**, or set the value to **0** in order to disable the timeout mechanism completely.

To disconnect from the VPN, click on the **Disconnect** button.

Alternatively, you can connect and disconnect from the Astaro Secure Client **tray icon** menu. Click on the icon with the right mouse button, and you will see the context menu.

If the connection is established successfully, you can see the **tray icon** switching from red to green, as can be seen in right screenshot.

The way to set-up the Astaro Secure Client is described in the associated **ASC V8.3 User Manual** or **ASC V8.3 Configuration Guide**.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

SOPHOS