2.2. Configuration of the Remote Client

2.2.1. Astaro User Portal: Getting Software and Certificates

The **Astaro User Portal** is available for the remote access users. You can use this portal to download guides and tools for the configuration of your client. Especially for the SSL remote access, the user portal offers a configuration guide and a customized SSL VPN client software, which already includes software, certificates and configuration handled by a simple installation procedure. This client supports most business applications such as native Outlook, native Windows Filesharing and many more. 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).
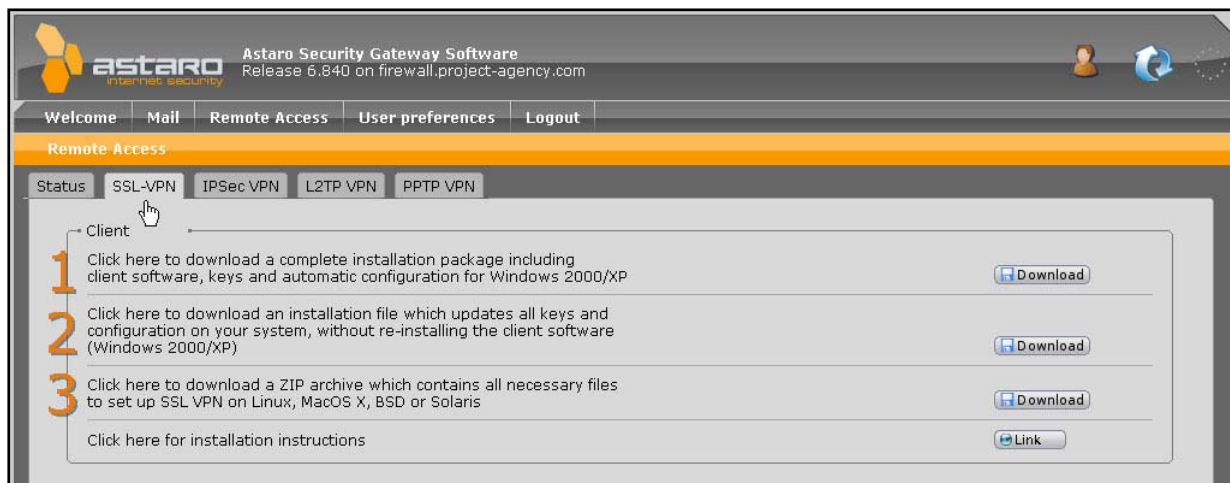
2. **Log in to the Astaro UserPortal:**

   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 SSL Remote Access to your client:**

   The **SSL VPN** tab will contain the software and keys for your client; to do so have two options. Either you download (see item 1) a complete software package with the pertinent

key for a new installation or you update an already installed SSL VPN client (see item 2) with new keys. The SSL VPN Client is available for Microsoft Windows 2000 and XP.

Start the download process by clicking on **Download**.

For the configuration of *SSL VPN* on Linux, MacOS X, BSD and Solaris please see installation instructions on http://openvpn.net (all necessary files are available over the Astaro User Portal, see item 3).

Close the *Astaro User Portal* session by clicking on **Logout**.

The rest of the configuration takes place on the remote user client. This will require the IP address or hostname of the server, as well as a valid username and password. These should be supplied by the security system administrator.
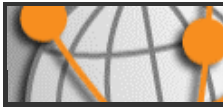
## 2.2.2.   SSL VPN Client: Installing the Software

The first part of the installation uses the Installation Menu to configure basic settings. The setup program will check the hardware of the system, and then install the necessary software on your PC.

Unpack the installation package (for example by using WinZip), if you have received it as a .ZIP file. Open a file browser and go to the appropriate directory. Launch the file **setup.exe** from this directory.
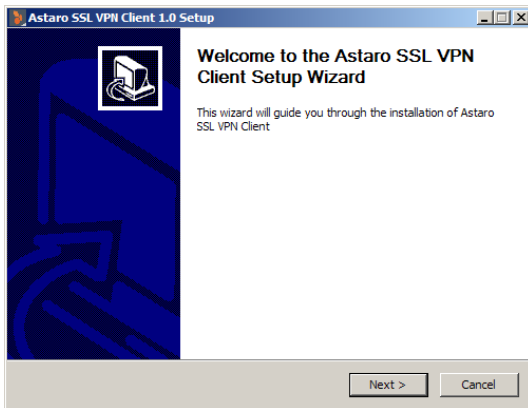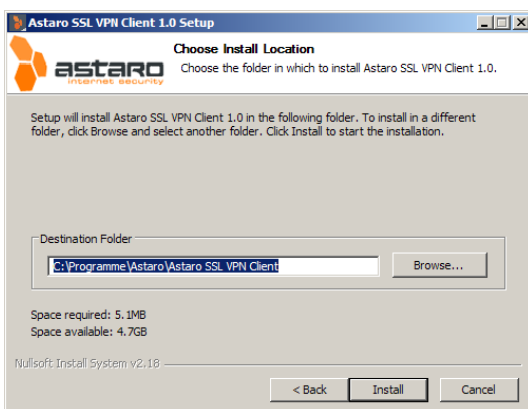

You should see the installation wizard now.
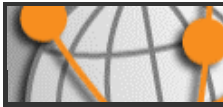
Click on **Next** to proceed.
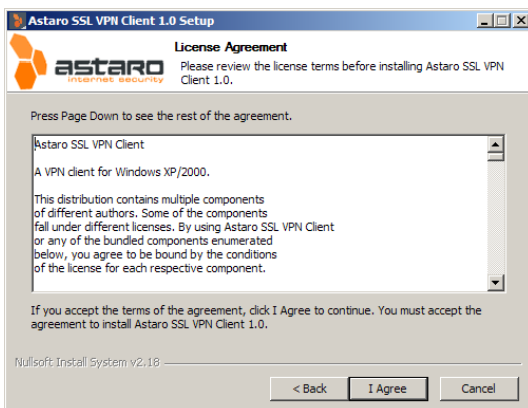
You will see the software license.

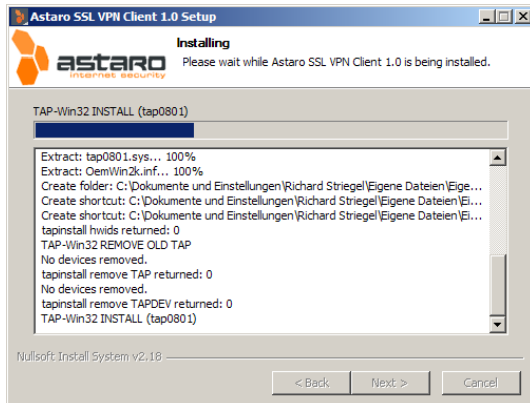If you agree to the terms of the license, click on **I Agree**.
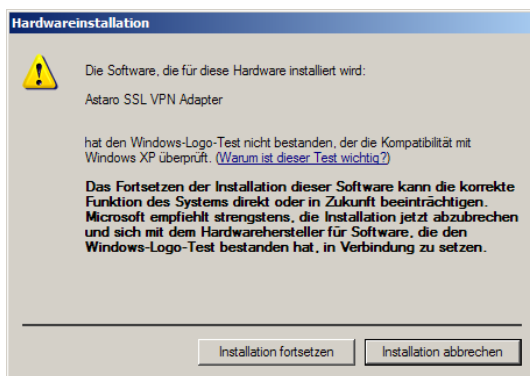

Choose the install location.

Click on **Install** to proceed.
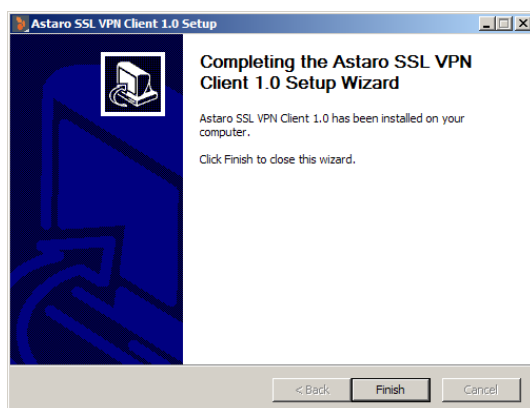
Then the installation process will be started.

The installation wizard will copy the necessary files on your system. A virtual network card will be installed during the installation process. Since the relevant driver is not certified by Microsoft, a corresponding caution message will appear during the installation process. You can ignore this message.

Click on **Continue Installation**.
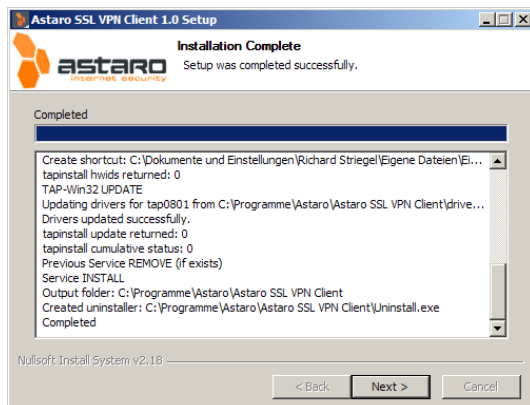
When installation process is finished, you are asked to complete. Click on **Next** to do so.

When installation process is finished, you are asked to close the installation wizard. Click on **Finish** to do so.

After the software installation the client is automatically started. Then the **SSL VPN** icon ( ) will be displayed in your Task bar. A double click on this icon opens the **User Authentication** dialogue box.
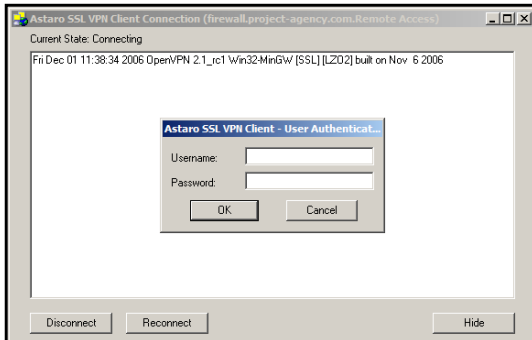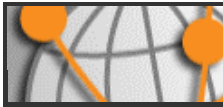
Log in with your **Username** and **Password**, which you use also for the **Astaro User Portal** and then start the connection by clicking **OK**.

The connection status is indicated by the *SSL VPN* icon: Disconnected ( ), connecting ( ) and connected ( ).

The **Connection** dialogue box allows you to monitor the set-up of the connection. The SSL VPN Remote Access can be disconnected by clicking **Disconnect**.

Further information is usually available from the network administrator.

The basic settings for the remote access via SSL are now finished. Depending on the security policy of your organization and the requirements of your network you might have to make additional settings.