

**SOPHOS**

Security made simple.

# Sophos UTM

## Remote Access via SSL

## Configuring Remote Client

Product version: 9.300

Document date: Tuesday, October 14, 2014



The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of Sophos Limited. Translations of this original manual must be marked as follows: "Translation of the original manual".

© 2014 Sophos Limited. All rights reserved.

<http://www.sophos.com>

Sophos UTM, Sophos UTM Manager, Astaro Security Gateway, Astaro Command Center, Sophos Gateway Manager, Sophos iView Setup and WebAdmin are trademarks of Sophos Limited. Cisco is a registered trademark of Cisco Systems Inc. iOS is a trademark of Apple Inc. Linux is a trademark of Linus Torvalds. All further trademarks are the property of their respective owners.

## Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to [nsg-docu@sophos.com](mailto:nsg-docu@sophos.com).

# Contents

<b>1 Introduction</b>	<b>4</b>
<b>2 Configuring a Remote Computer</b>	<b>5</b>
2.1 Getting Software and Certificates .....	5
2.2 Installing the SSL VPN Client Software .....	6
2.3 Connecting to the VPN .....	9
<b>3 Configuring a Mobile Device</b>	<b>11</b>

# 1 Introduction

To be able to access the UTM via SSL VPN, you need to configure your remote client. To do so, access the UTM User Portal with a browser on the remote client. There, the necessary installation instructions, software and/or configuration files are available for download.

For remote computers, the SSL VPN client software including configuration is available. The client software has to be installed once for the remote client to be able to connect.

For iOS or Android devices, a VPN configuration is available that can be installed on an OpenVPN software.

## 2 Configuring a Remote Computer

On the remote computer, the allowed user downloads the Sophos SSL VPN Client software including configuration data from the UTM User Portal. After installing the software package on the remote client, the SSL VPN connection can be opened.

### 2.1 Getting Software and Certificates

The UTM User Portal is available to all remote access users. From this portal, you can download guides and tools for the configuration of your client. You should get the following user credentials for the User Portal from your system administrator: IP address, username, and password.

Especially for 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 file sharing, and many more.

1. **Start your browser and open the User Portal.**

Start your browser and enter the management address of the User Portal as follows:

`https://IP address (example: https://218.93.117.220).`

A security note will be displayed.

Accept the security note. Depending on the browser, click *I Understand the Risks > Add Exception > Confirm Security Exception* (Mozilla Firefox), or *Proceed Anyway* (Google Chrome), or *Continue to this website* (Microsoft Internet Explorer).

2. **Log in to the User Portal.**

Enter your credentials:

**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.

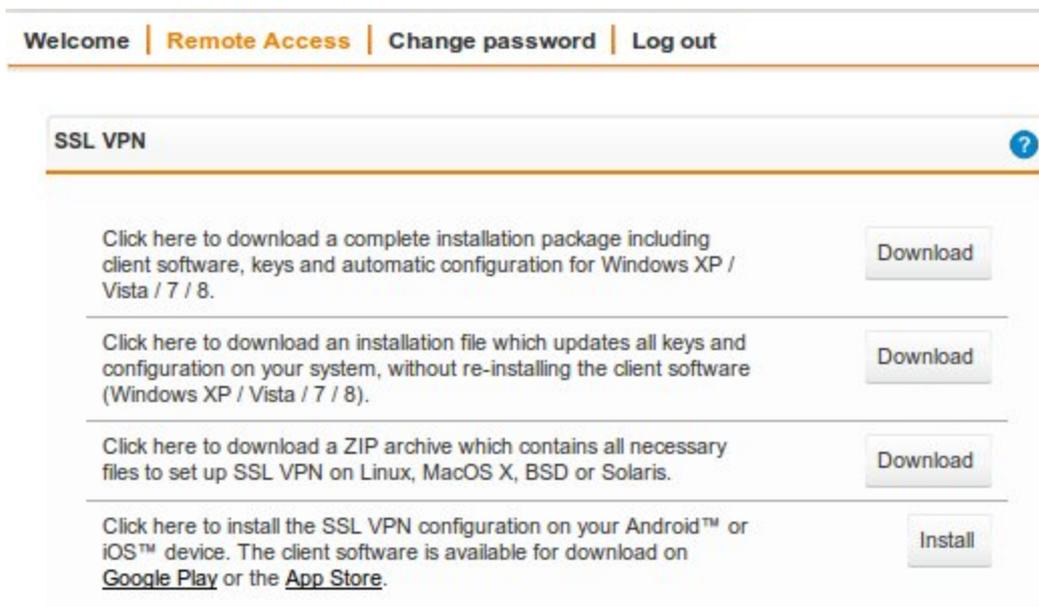
Click *Login*.

3. **On the *Remote Access* page, download the tools and/or configuration guide for setting up your remote access connection.**

This page can contain up to five sections, depending on the remote access connection types (IPsec, SSL, L2TP, PPTP, iOS devices) your administrator enabled for you.

At the top of most of the sections you find a help icon which opens the respective remote access guide.

## 2 Configuring a Remote Computer



In the *SSL VPN* section, you can download the client software. With the topmost button, you download a complete software package with the pertinent key for a new installation. With the second button, you update an already installed SSL VPN client with new keys.

The third button provides all necessary files for the configuration of SSL VPN on Linux, MacOS X, BSD, and Solaris.

**Cross Reference** – For the configuration of SSL VPN on Linux, MacOS X, BSD, and Solaris please see installation instructions on <http://openvpn.net>.

Start the download process by clicking *Download*.

#### 4. Close the User Portal session by clicking *Log out*.

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, which should be supplied by the system administrator.

## 2.2 Installing the SSL VPN Client Software

The setup program will check the hardware of the system, and then install the necessary software on your PC.

### 1. Unpack the installation package.

If you have received it as a .zip file, unpack the installation package, for example by using WinZip.

### 2. Start the installation.

Open a file browser and go to the location of the installation file *setup.exe*. Launch the file from this directory.

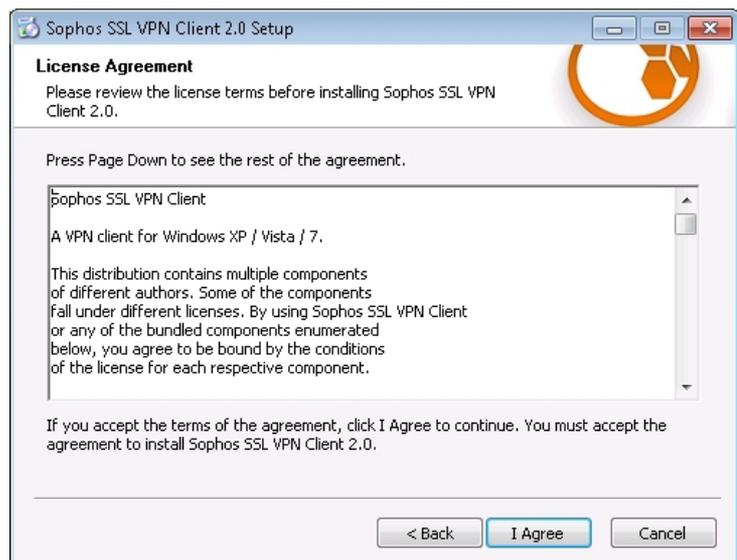
The installation wizard should start up now.

Click *Next* to proceed.



### 3. Accept the software license agreement.

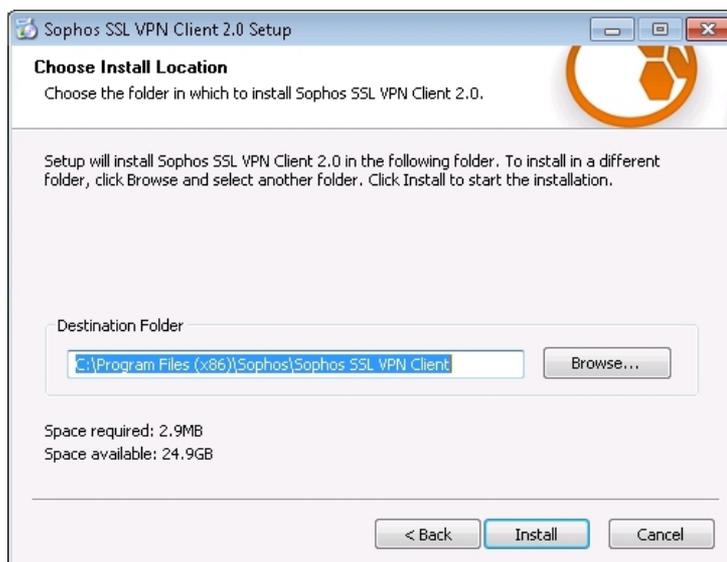
If you agree to the terms of the license, click *I Agree*.



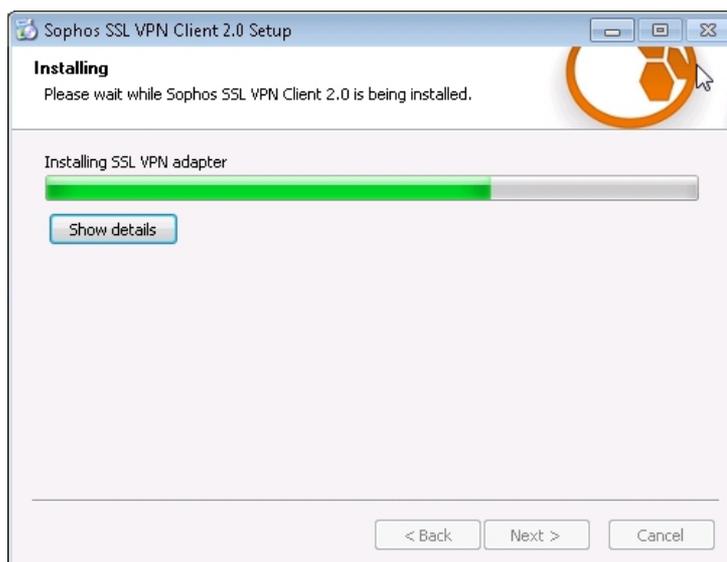
### 4. Choose the install location.

## 2 Configuring a Remote Computer

Click *Browse*, select the appropriate directory, and click *OK*.



5. **Click *Install* to proceed.**  
The installation process will be started.



6. **Confirm the warning message.**  
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.

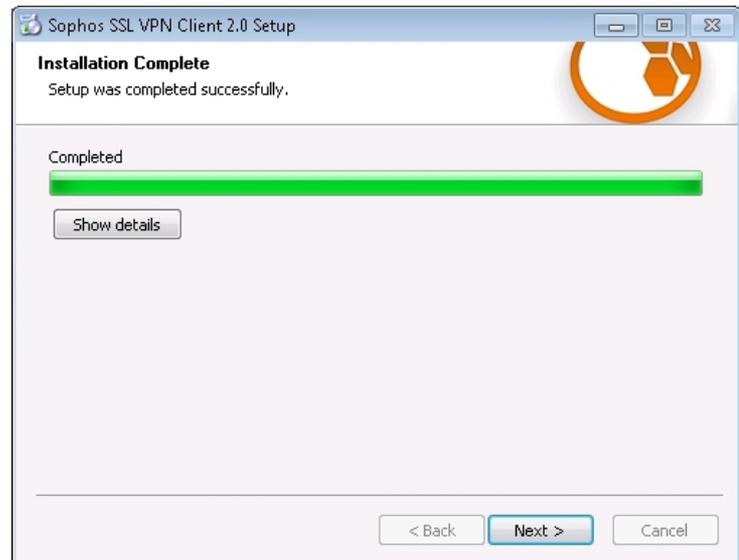
Click *Install*.

7. **Confirm the completion message.**



When the installation process is finished, a completion message is displayed.

Click *Next* to confirm it.

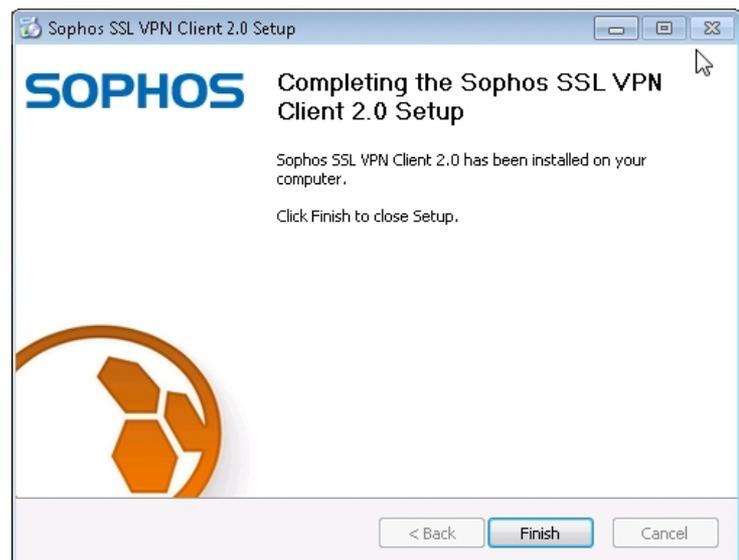


### 8. Finish the installation by clicking *Finish*.

After the software installation the client is automatically started.

Then the SSL VPN icon  will be displayed in your task bar.

Further information is usually available from the network administrator.



## 2.3 Connecting to the VPN

### 1. Open the User Authentication dialog box.

Double-click the SSL VPN task bar icon  to open the *User Authentication* dialog box.

In case you have more than one connection specified, right-click the icon to open a list of available connections.



### 2. Log in.

Log in with your username and password, which you use also for the User Portal, and then start the connection by clicking *OK*.

## 2 Configuring a Remote Computer

---

The connection status is indicated by the *SSL VPN* icon: disconnected () , connecting () , and connected () . The *Connection* dialog box allows you to monitor the set-up of the connection.

The *SSL VPN* remote access can be disconnected by clicking *Disconnect* in the context menu of the task bar icon.

# 3 Configuring a Mobile Device

On the mobile device, prior to installing the configuration, the appropriate OpenVPN client software has to be installed on your device. It can be downloaded via the appropriate link: [Google Play](#) or [App Store](#).

Then, the allowed user downloads the configuration from the UTM User Portal. The UTM User Portal is available to all remote access users. From this portal, you can download guides and tools for the configuration of your client. You should get the following user credentials for the User Portal from your system administrator: IP address, username, and password.

1. **On the mobile device, start your browser and open the User Portal.**

Start your browser and enter the management address of the User Portal as follows:

`https://IP address (example: https://218.93.117.220)`.

A security note will be displayed.

Accept the security note.

2. **Log in to the User Portal.**

Enter your credentials:

**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. **On the *Remote Access* page, download the configuration for setting up your SSL VPN connection.**

This page can contain up to five sections, depending on the remote access connection types your administrator enabled for you.

### 3 Configuring a Mobile Device

---

Welcome | **Remote Access** | Change password | Log out

---

#### SSL VPN ?

---

Click here to download a complete installation package including client software, keys and automatic configuration for Windows XP / Vista / 7 / 8.	Download
Click here to download an installation file which updates all keys and configuration on your system, without re-installing the client software (Windows XP / Vista / 7 / 8).	Download
Click here to download a ZIP archive which contains all necessary files to set up SSL VPN on Linux, MacOS X, BSD or Solaris.	Download
Click here to install the SSL VPN configuration on your Android™ or iOS™ device. The client software is available for download on <a href="#">Google Play</a> or the <a href="#">App Store</a> .	Install

In the *SSL VPN* section, Click the *Install* button.

4. **Follow the instructions on the mobile device.**

Open the configuration with the OpenVPN software and add the configuration there.

5. **Close the User Portal session by clicking *Log out*.**

Now you should be able to connect via SSL VPN.