SOPHOS

Security made simple.

# Sophos UTM

## Remote Access via L2TP

## Configuring Remote Client

Product version: 9.300

Document date: Tuesday, October 14, 2014

# 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.

# Contents

# 1 Introduction

To be able to access the UTM via L2TP over IPsec VPN, you need to configure your remote computer. To do so, access the UTM User Portal with a browser on the remote client. There, the necessary installation instructions and the preshared key or the certificate are available for download. Then you configure the VPN connection on Windows.

# 2 Getting a Preshared Key or Certificate

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 the L2TP remote access with authentication based on *Preshared key*, the User Portal offers the shared secret. For authentication with *X.509 certificate*, the User Portal offers the necessary certificate.

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:

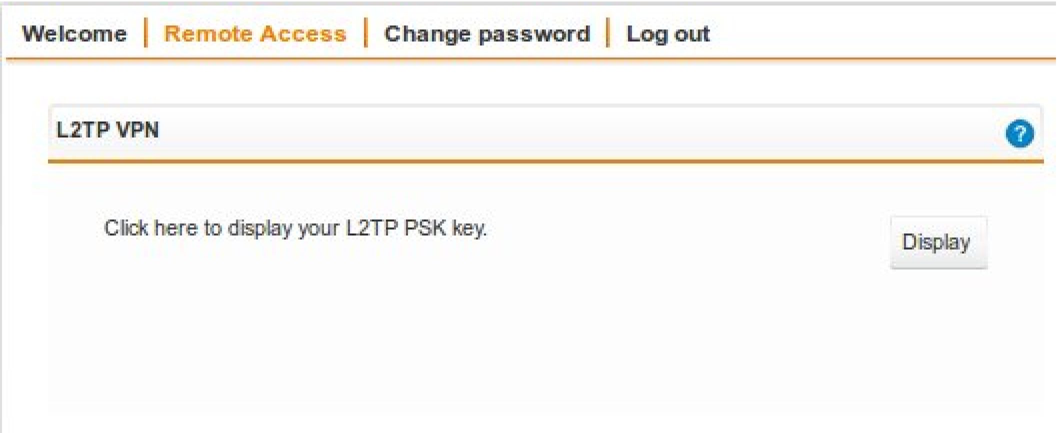
   **Username:** Your username, which you received from the administrator.

   **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.



Click here to display your L2TP PSK key.

The available data depends on the authentication mode configured by the administrator. With preshared key, click the *Display* button to see the preshared key. Otherwise, a certificate is available. In the *Export password* field, enter a password to secure the PKCS#12 container before downloading the certificate. Note that you will need the security password of the certificate later on.

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

The rest of the configuration takes place on the remote user client. This step will require the IP address or hostname of the server, which should be supplied by the system administrator.

# 3 Using a Preshared Key

This chapter describes the configuration of Microsoft Windows XP/Vista/7 for using a preshared key as L2TP over IPsec authentication.

## 3.1 Configuring Windows Vista or 7

1. **Click *Start* and then *Control Panel*.**
2. **In the Control Panel, click *Network and Internet*, then *Network and Sharing Center*.**
3. **Click *Set up a new connection or network*.**
   The *Set up a Connection or Network* wizard opens.
4. **Click *Connect to a workplace* and *Next*.**
5. **Define the dial-up Internet connection.**
   If you have a permanent connection to the Internet, select the *Use my Internet connection (VPN)* option. Otherwise, click *Dial directly*, and then select your dial-up Internet connection from the list.
6. **Click *Next*.**
7. **Enter the hostname or the IP address of the gateway.**
   Enter the hostname or the IP address of the gateway that you want to connect to, and enter a descriptive name for the connection. Consider the following options:

   **Allow other people to use this connection:** Select this option if you want the connection to be available to anyone who logs on to the client.

   **Don't connect now; just set it up so I can connect later:** Select this option.
8. **Click *Next*.**
9. **Enter the user credentials.**
   Enter the *User name* and *Password* (*Remote User Account*).
10. **Click *Create*.**
    The wizard closes.
11. **In the *Network and Sharing Center*, click *Connect to a network*.**
    A list with the available network connection opens.
12. **Right-click the new connection and select *Properties*.**
    The *Connection Properties* dialog box opens.
13. **Only for Windows Vista, do the following:**
    1. **Select the *Networking* tab.**
    2. **In the *Type of VPN* section, select *L2TP IPsec VPN*.**
    3. **Click the *IPsec Settings* button.**

Select *Use preshared key for authentication*, enter the *Preshared Key*, and click *OK*.

4. **Select the *Security* tab.**
5. **Select the *Advanced (custom settings)* option and click the *Settings* button.**
6. **Set the *Data encryption* option to *Optional encryption (connect even if no encryption)*.**
7. **Click *OK*.**

14. **Only for Windows 7, do the following:**
    1. **Select the *Security* tab.**
    2. **In the *Type of VPN* section select *Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)*.**
    3. **Click the *Advanced settings* button.**
       Select *Use preshared key for authentication*, enter the *Preshared Key*, and click *OK*.
    4. **Set the *Data encryption* option to *Optional encryption (connect even if no encryption)*.**
15. **To close the dialog box, click *OK*.**
    Now you can directly establish the connection with your username and password in the login window.

    How to establish the connection if the login window is not open is described in chapter Connecting to the VPN.

## 3.2 Configuring Windows XP

1. **Click *Start* > *Settings*, and then click *Control Panel*.**
2. **In the Control Panel, double-click *Network Connections*.**
   The *Network Connections* window opens.
3. **Click *Create a new connection*.**
   The *New Connection Wizard* window opens.
4. **Click *Next*.**
5. **Click *Connect to the network at my workplace* and then *Next*.**
6. **Define how to connect to your network.**
   Select *Virtual Private Network connection* if you use a VPN connection over Internet.
7. **Click *Next*.**
8. **Enter the name of the company or a descriptive name for the connection.**
9. **Click *Next*.**
10. **Define the dial-up Internet connection.**

If you have a permanent connection to the Internet, select the *Do not dial the initial connection* option. Otherwise, click *Automatically dial this initial connection*, and then select your dial-up Internet connection from the list.

11. **Click *Next*.**
12. **Enter the hostname or the IP address of the gateway that you want to connect to.**
13. **Click *Next*.**
14. **Select who should be able to use this connection.**
    Click *Anyone's use* if you want the connection to be available to anyone who logs on to the client. Otherwise, click *My use only*, to make the connection only available for your account.
15. **Click *Next*.**
16. **If you want to create a shortcut on the desktop, click *Add a shortcut to this connection to my desktop*.**
17. **Click *Finish*.**
    The login window opens.
18. **In the login window, click *Properties*.**
    The *Properties* dialog box opens.
19. **Open the *Security* tab.**
20. **Disable the *Require data encryption (disconnect if none)* option.**
21. **Click *IPsec Settings*.**
22. **Select *Use pre-shared Key for authentication* and enter the preshared key.**
23. **Click *OK*.**
24. **Open the *Networking* tab.**
25. **In the *Type of VPN* section, select *L2TP IPsec VPN*.**
26. **To close the dialog box, click *OK*.**
    Now you can directly establish the connection with your username and password in the login window.

    How to establish the connection if the login window is not open is described in chapter Connecting to the VPN.

# 4 Using a Certificate

This chapter describes the configuration of Microsoft Windows XP/Vista/7 for using X.509 certificates as IPsec authentication. The configuration is generated in two steps:

## 4.1 Importing a Certificate into Microsoft Windows XP, Vista, or 7

1. **Start the management console.**
   - **In Windows Vista or 7, click *Start*, then, in the *Search* field, enter *mmc*.**
     The program *mmc* is displayed in the *Programs* list.

     Click the *mmc* entry.

     Depending on your settings, you need to confirm with *Yes* or *Continue*. The management console opens.
   - **In Windows XP, click *Start* > *Run*. Enter `mmc` and click *OK*.**
2. **From the menu, select *File* > *Add/Remove Snap-in*.**
3. **Click *Add*.**
4. **Select *Certificates*, then click *Add*.**
5. **Select *Computer account*, then click *Next*.**
6. **Select *Local computer (the computer this console is running on)*.**
7. **Click *Finish*, then *Close*, and then *OK*.**
8. **In the tree view on the left side, in the category *Certificates (Local Computer)*, right-click *Personal*.**
9. **From the context menu select *All Tasks* > *Import*.**
   The *Certificate Import Wizard* opens.
10. **Click *Next*.**
11. **Select *Browse* and select the *PKCS#12 container file* to import.**
    You might have to select the correct file extension .p12 in the drop-down list to be displayed the PKCS#12 container files.
12. **Click *Next*.**
13. **Enter the security password.**
    Enter the security password of the certificate that you used while downloading the certificate from the User Portal.
14. **Click *Next*.**
15. **Select *Automatically select the certificate store based on the type of certificate*.**
16. **Click *Next* and then *Finish*.**

17. **Select *Action* > *Refresh*.**
    Now, the newly imported certificate should be visible.
18. **Close the management console.**
    If asked whether you want to save anything, you don’t need to.
19. **Move the CA certificate to the root CA folder, if necessary.**

## 4.2 Configuring Windows Vista or 7

1. **Click *Start* and then *Control Panel*.**
2. **In the Control Panel, click *Network and Internet*, then *Network and Sharing Center*.**
3. **Click *Set up a new connection or network*.**
   The *Set up a Connection or Network* wizard opens.
4. **Click *Connect to a workplace* and *Next*.**
5. **Define the dial-up Internet connection.**
   If you have a permanent connection to the Internet, select the *Use my Internet connection (VPN)* option. Otherwise, click *Dial directly*, and then select your dial-up Internet connection from the list.
6. **Click *Next*.**
7. **Enter the hostname or the IP address of the gateway.**
   Enter the hostname or the IP address of the gateway that you want to connect to, and enter a descriptive name for the connection. Consider the following options:

   **Allow other people to use this connection:** Select this option if you want the connection to be available to anyone who logs on to the client.

   **Don't connect now; just set it up so I can connect later:** Select this option.
8. **Click *Next*.**
9. **Enter the user credentials.**
   Enter the *User name* and *Password* (*Remote User Account*).
10. **Click *Create*.**
    The wizard closes.
11. **In the *Network and Sharing Center*, click *Connect to a network*.**
    A list with the available network connection opens.
12. **Right-click the new connection and select *Properties*.**
    The *Connection Properties* dialog box opens.
13. **Only for Windows Vista, do the following:**
    1. **Select the *Networking* tab.**
    2. **In the *Type of VPN* section, select *L2TP IPsec VPN*.**
    3. **Select the *Security* tab.**

   4. **Select the *Advanced (custom settings)* option and click the *Settings* button.**
   5. **Set the *Data encryption* option to *Optional encryption (connect even if no encryption)*.**
   6. **Click *OK*.**

14. **Only for Windows 7, do the following:**
    1. **Select the *Security* tab.**
    2. **In the *Type of VPN* section select *Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)*.**
    3. **Set the *Data encryption* option to *Optional encryption (connect even if no encryption)*.**
15. **To close the dialog box, click *OK*.**
    Now you can directly establish the connection with your username and password in the login window.

    How to establish the connection if the login window is not open is described in chapter Connecting to the VPN.

## 4.3 Configuring Windows XP

1. **Click *Start* > *Settings*, and then click *Control Panel*.**
2. **In the Control Panel, double-click *Network Connections*.**
   The *Network Connections* window opens.
3. **Click *Create a new connection*.**
   The *New Connection Wizard* window opens.
4. **Click *Next*.**
5. **Click *Connect to the network at my workplace* and then *Next*.**
6. **Define how to connect to your network.**
   Select *Virtual Private Network connection* if you use a VPN connection over Internet.
7. **Click *Next*.**
8. **Enter the name of the company or a descriptive name for the connection.**
9. **Click *Next*.**
10. **Define the dial-up Internet connection.**
    If you have a permanent connection to the Internet, select the *Do not dial the initial connection* option. Otherwise, click *Automatically dial this initial connection*, and then select your dial-up Internet connection from the list.
11. **Click *Next*.**
12. **Enter the hostname or the IP address of the gateway that you want to connect to.**
13. **Click *Next*.**

14. **Select who should be able to use this connection.**
    Click *Anyone's use* if you want the connection to be available to anyone who logs on to the client. Otherwise, click *My use only*, to make the connection only available for your account.
15. **Click *Next*.**
16. **If you want to create a shortcut on the desktop, click *Add a shortcut to this connection to my desktop*.**
17. **Click *Finish*.**
    The login window opens.
18. **In the login window, click *Properties*.**
    The *Properties* dialog box opens.
13. **Open the *Security* tab.**
14. **Disable the *Require data encryption (disconnect if none)* option.**
15. **Open the *Networking* tab.**
16. **In the *Type of VPN* section select *L2TP IPsec VPN*.**
17. **To close the dialog box, click *OK*.**
    Now you can directly establish the connection with your username and password in the login window.

    How to establish the connection if the login window is not open is described in chapter Connecting to the VPN.

# 5 Connecting to the VPN

When the connection is configured and the login window is closed, you can establish the connection as follows:

1. **Open the connections list.**
   In Windows Vista or 7, in the *Network and Sharing Center*, click *Connect to a network*. A list of available network connections opens.

   Alternatively, in Windows Vista, click *Start* > *Connect To*. Or, if you added a connection shortcut to the desktop, just double-click the shortcut on the desktop.

   Alternatively, in Windows 7, click the Network Connection icon on the right of the task bar.

   In Windows XP, the *Network Connections* window shows a list of available VPN connections.

2. **Initiate the connection.**
   In Windows Vista or 7, in the network connections list, click the appropriate connection. In Windows XP, right-click the connection and select *Connect*.

   If you are not currently connected to the Internet, MS Windows offers to connect to the Internet. After your computer connects to the Internet, the VPN server prompts you for your username and password.

3. **Type your username and password, and then click *Connect*.**
   Your network resources should be available to you just like they are when you connect directly to the network.

To disconnect from the VPN, right-click the Network Connection icon on the right of the task bar, then click *Disconnect from* and select the connection.

Further information is usually available from the network administrator.