USER GUIDE

WWPass Security for VPN (OpenVPN)

TABLE OF CONTENTS

CHAPTER 1 — WELCOME

This chapter introduces WWPass Security for VPN (OpenVPN) and provides information on using a PassKey™ from WWPass, accessing related documentation, and contacting WWPass Product Support.

.

Topics In This Chapter

Introducing WWPass Security for VPN (OpenVPN)

This user guide covers how to set up and use WWPass Security for VPN (OpenVPN), the WWPass authentication solution for OpenVPN.

WWPass Security for VPN (OpenVPN) allows you to log into OpenVPN using a PassKey instead of a username and password. The solution is available for Windows and Linux.

Note: WWPass Security for VPN (OpenVPN) is part of the WWPass Security Pack™ and is shown in the WWPass Dashboard™. The Security Pack allows you to activate a PassKey and use WWPass authentication solutions. Dashboard shows you the solutions included in the Security Pack.

Connecting Your PassKey to Your Computer

To use your PassKey, you connect it to your computer and enter your access code, if prompted for this.

Your PassKey is NFC and USB enabled. You can place your PassKey on an NFC reader or insert the PassKey into a computer USB port.

Enter your access code using exactly the same characters and cases (upper or lower) it was created with.

You are given three chances to enter the correct code. If you enter the access code incorrectly three times in a row, your PassKey is locked for 15 minutes and cannot be used.

Need Assistance?

If you encounter a problem or have a question, you can contact the WWPass Service Desk as follows:

Phone	1-888-WWPASS0 (+1-888-997-2770)
Email	info@wwpass.com

Report a Problem from the Dashboard

An easy way to report a problem is to email the Service Desk directly from the WWPass Dashboard, included in WWPass Security Pack.

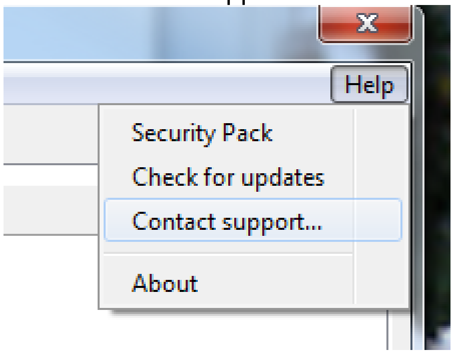
The email identifies version numbers for your Security Pack and operating system. In addition, the current logs for WWPass software are automatically attached to the email.

Logs contain information that can help Product Support troubleshoot any problem you experience. For example, logs contain information such as actions and their times, and services accessed. Actions include PassKey authentication for login, email signing, and email decryption.

On Windows, logs are located in Users\username and Program Data. On Linux, logs are located in HOME. Logs should not be changed before they are sent to Product Support.

To report a problem from the Dashboard

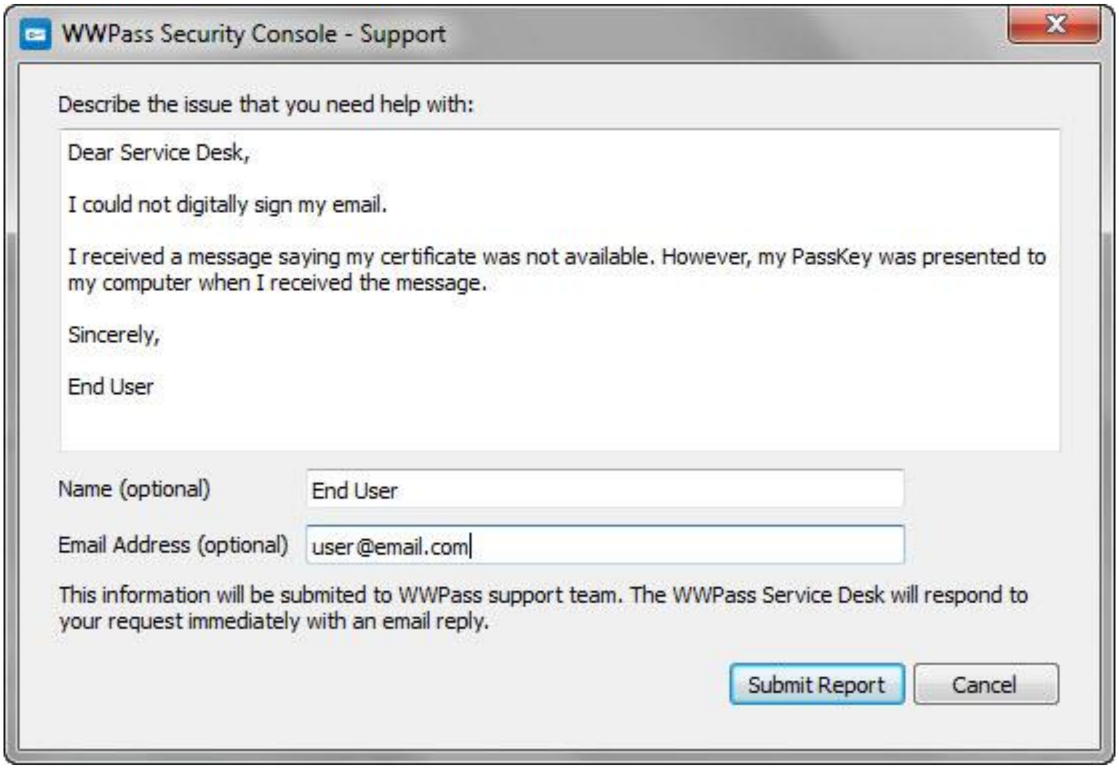
1. Select “Contact Support…” from the Dashboard Help menu.



2. In the Support window that opens, type a description of the problem you need help with. You can also enter a question.

3. Enter the email address Product Support should reply to and enter your name.

4. Click Submit Report to send your report along with the current version of all available logs.



Describe the issue that you need help with:

Dear Service Desk,

I could not digitally sign my email.

I received a message saying my certificate was not available. However, my PassKey was presented to my computer when I received the message.

Sincerely,

End User

Name (optional): End User

Email Address (optional): user@email.com

This information will be submited to WWPass support team. The WWPass Service Desk will respond to your request immediately with an email reply.

CHAPTER 2 — REQUIREMENTS

Requirement	Details
OpenVPN Client	OpenVPN version 2.3.2 or higher 32-bit is supported. The 32-bit client can be used on 32-bit and 64-bit systems: • To install OpenVPN for Windows, download and run the OpenVPN installer: http://openvpn.net/index.php/open-source/downloads.html • To install OpenVPN for Linux (Ubuntu), run this command: `sudo apt-get install openvpn` The OpenVPN client is installed on your computer and needs access to an OpenVPN server.
Personal certificate for OpenVPN	This is a digital X.509 certificate from a Certificate Authority (CA). It serves as a credential that authenticates your identity when you log into OpenVPN with a PassKey. You can obtain a certificate from a third-party such as Comodo or from a system administrator.
Certificate Authority (CA) certificate	This is a “root” certificate that verifies your personal certificate for OpenVPN. Contact a system administrator to obtain a CA certificate. Then create a folder called "certs" under your OpenVPN folder and save the certificate file in that folder: • For 32-bit OpenVPN on 32-bit or 64-bit Windows use: C:\Program Files\OpenVPN\certs • For 64-bit OpenVPN on 64-bit Windows use: C:\Program Files (x86)\OpenVPN\certs • For Linux use: /etc/ssl/certs/
WWPass KeySet	This includes the PassKey used for authentication when you log in to OpenVPN. Click here for more information.
WWPass Software	This allows you to activate a KeySet and use WWPass Security for VPN (OpenVPN): • For personal use, install the WWPass Security Pack. Click here for more information. • For use at an enterprise with a Windows network, install WWPass Security Pack. To obtain the pack, contact your system administrator or sales at WWPass: 1-888-997-2771

Requirement	Details
Web browser	This is needed to activate your KeySet and authenticate with your PassKey. You might also need a browser to download a certificate from a third-party CA such as Comodo: • For authentication and Key Activation, you can use browsers supported for your operating system. Click here to see a list. • For downloading a certificate, use Firefox (on Windows, Mac or Linux) or Internet Explorer (on Windows). Click here to download Firefox.
Internet access	Outbound TCP connections must be allowed from your computer to ports 80 (HTTP) and 443 (HTTPS).

CHAPTER 3 — SETUP

This chapter covers how to set up for PassKey login on OpenVPN.

Topics in this Chapter

Smart Start for Setup

The Smart Start below identifies all setup steps for WWPass Security for VPN (OpenVPN). If detailed information about a step is available, a link to the information is provided.

Smart Start

1. Install the WWPass Security Pack. Click here for more information.

2. Obtain and activate your KeySet. Click here for more information. (If you are currently using another WWPass solution, your KeySet is already activated.)

3. Obtain a certificate for OpenVPN from a third-party such as Comodo or from a system administrator. When you download a certificate, use the Web browser required for your system:

   - On Mac or Linux, use Firefox
   - On Windows, use Firefox or Internet Explorer

   Also obtain a Certificate Authority certificate for OpenVPN, create a "certs" folder under your OpenVPN folder and save the Certificate Authority certificate in "certs". For more information about certificates, see Requirements.

4. If your OpenVPN certificate is available in a file, import the certificate for use with your PassKey.

5. Install the 32-bit OpenVPN client as follows:

   - To install OpenVPN for Windows, download and run the OpenVPN installer: http://openvpn.net/index.php/open-source/downloads.html
   - To install OpenVPN for Linux (Ubuntu), run this command:

     ```
     sudo apt-get install openvpn
     ```

6. Obtain an OpenVPN executable (openvpn-gui-1.0.3-pkcs11.exe) that supports the Cryptographic Token Interface Standard used for PassKey authentication into OpenVPN:

   a) Go to this site: http://ziggurat29.com/

   b) Scroll to this link: **OpenVPN GUI with pkcs11 support**. Then click the link to download a Zip folder with the executable.

   c) Extract the executable from its Zip folder and create a desktop shortcut for the executable.

7. Configure the OpenVPN client.

Import a Certificate for Use with Your PassKey

Depending on how you obtain an OpenVPN certificate, it might be available in a file. In this case, you can follow the steps below to import the certificate for use with your PassKey. Certificate files typically have a .pfx or .p12 extension.

Steps are performed with the WWPass Dashboard, which is installed as part of WWPass Security Pack.

Before you import a certificate:

- Put the certificate file in a temporary location on your computer.
- If the file is encrypted, make sure you know the password that was used to encrypt the file.

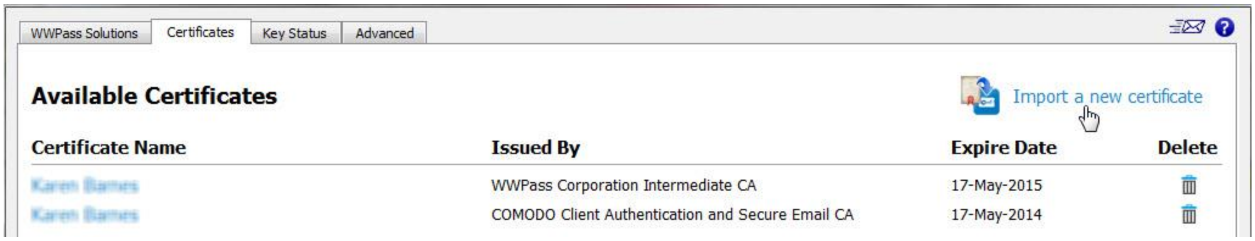
After you import a certificate:

- Remove the certificate file from your computer. At this point, the certificate is securely stored in WWPass cloud storage, where it is encrypted, fragmented, and dispersed.

Note: See the Smart Start for a list of all steps in the setup process.

To import a certificate

1. Connect your PassKey to your computer.
2. Open the WWPass Dashboard. The Dashboard is identified by the WWPass Key icon.
3. From the Certificates tab, click **Import a new certificate**.



Available Certificates

Certificate Name	Issued By	Expire Date	Delete
[redacted]	WWPass Corporation Intermediate CA	17-May-2015	🗑
[redacted]	COMODO Client Authentication and Secure Email CA	17-May-2014	🗑

4. From the Open Certificate window, locate the certificate file. Look for an extension of .pfx or .p12. Select the file and click Open.
5. If prompted for the password used to encrypt the certificate file, enter the password and click OK.
6. Enter the access code for your PassKey and click OK. The certificate is imported and shown in the Dashboard's Certificates tab.

Configure the OpenVPN Client

Follow the steps below to configure the OpenVPN client for authentication with your PassKey.

These steps create a configuration file that is associated with your PassKey and OpenVPN certificate. If multiple users run OpenVPN from the same computer, each user needs their own configuration file on that computer. Configuration files are automatically stored in the OpenVPN folder.

Steps are performed with the WWPass Dashboard, which is installed as part of a WWPass Security Pack.

Before you begin:

- Obtain a personal certificate for OpenVPN and associate it with your PassKey. You can download a certificate from a third-party Certificate Authority such as Comodo or obtain one from a system administrator. If your certificate is available in a file, you can import the certificate for use with your PassKey.

- Also obtain a Certificate Authority certificate for OpenVPN, create a "certs" folder under your OpenVPN folder and save the Certificate Authority certificate in "certs". Contact a system administrator for assistance.

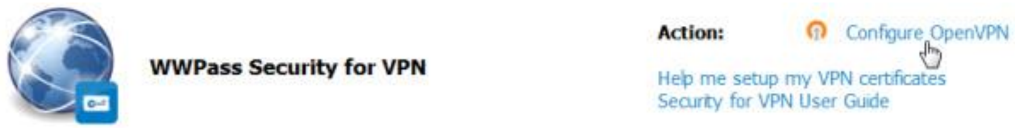
Note: See the Smart Start for a list of all steps in the setup process.

To configure the OpenVPN client

1. Connect your PassKey to your computer.

2. Open the WWPass Dashboard. The Dashboard is identified by the WWPass Key icon.

3. From the WWPass Solutions tab, click **Configure OpenVPN** next to WWPass Security for VPN. Then click Yes from the User Account Control message.


WWPass Security for VPN
Action:
Configure OpenVPN
Help me setup my VPN certificates
Security for VPN User Guide

4. From the WWPass Security for OpenVPN window, enter or select configuration settings as follows:

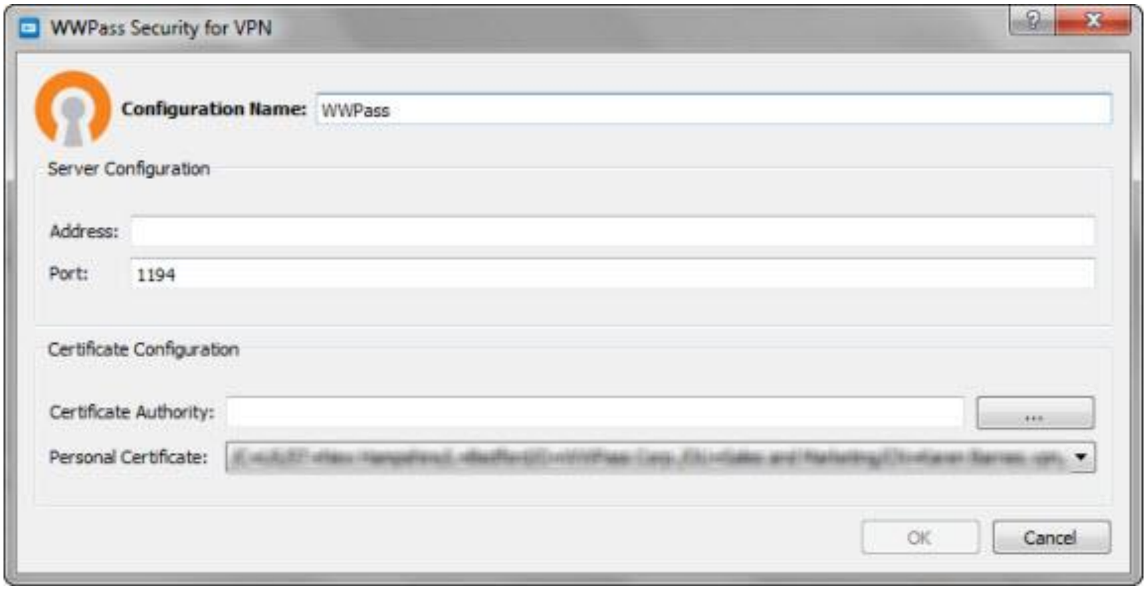
   - **Configuration Name:** Enter the name to use for the configuration file on Windows. You can specify a name for the file on Linux in the last step. To make it easy to identify your configuration file, include your own name in the file name, for example "WWPassVPNConfigJohn".

   - **Address:** Enter the hostname of your VPN server, for example, "OpenVPN.mycompany.com".

   - **Port:** Enter the port used by the OpenVPN client to communicate with the server if this is different from the official port (1194). The official port number is the default value.

   - **Certificate Authority:** Select the Certificate Authority (CA) certificate for OpenVPN. First, click [...]. Then select the certificate in the Select File window and click [Open ▾].

   - **Personal Certificate:** Select your personal certificate for OpenVPN. First, click the down arrow. Then click on your certificate in the list of certificates associated with your PassKey.



WWPass Security for VPN

Configuration Name: WWPass

Server Configuration

Address:

Port: 1194

Certificate Configuration

Certificate Authority:

Personal Certificate: [redacted]

5. Click [OK] in the WWPass Security for OpenVPN window. When the OpenVPN Configuration window displays the contents of the configuration file, click [Save] to save the file in the location shown at the top of the window. On Linux, also specify a name for the file. On Windows, the name entered in **Configuration Name** is automatically used as the file name.

CHAPTER 4 — USING A PASSKEY

This chapter covers how to use a PassKey to log into OpenVPN on Windows and Linux.

Topics In This Chapter

Use a PassKey to Log into OpenVPN on Windows

Follow the steps below to run OpenVPN from Windows and log in using your PassKey. You can run OpenVPN using a GUI client or the Windows Command Prompt.

To log in with your PassKey from the OpenVPN client

1) Connect your PassKey to your computer.
2) Double-click the desktop shortcut for the OpenVPN executable with PKCS11 support (openvpn-gui.exe). Administrator rights for the computer are needed.
3) Right-click the system tray icon for OpenVPN.
4) Select the Open VPN server to connect to and click **Connect**.
5) When prompted, enter your PassKey access code and click OK.

To log in with your PassKey from the Windows Command Prompt

1. Connect your PassKey to your computer.
2. Run the Windows Command Prompt as an administrator.
3. Start OpenVPN with one of the following commands, where name-of-config-file.ovpn is the name of the configuration file you created from the WWPass Dashboard, for example:

```
openvpn --config "c:\Program Files\OpenVPN\config\name-of-config-file.ovpn"
```

Use a PassKey to Log into OpenVPN on Linux

Follow the steps below to run OpenVPN from Linux and log in using your PassKey.

To log in with your PassKey on Linux

1. Connect your PassKey to your computer.

2. Start OpenVPN with the following command, where name-of-config-file.conf is the name of the configuration file you created from the WWPass Dashboard:

   ```
   sudo /usr/sbin/openvpn --config /etc/openvpn/name-of-config-file.conf
   ```

3. Enter the access code for your PassKey.

WWPass | 1155 Elm Street, Manchester, NH 03110 | Tel: +1.603.836.4932 or +1.888.997.2771 | www.wwpass.com