



USER GUIDE

WWPass Security for VPN (OpenVPN)

For WWPass Security Pack 2.6

May 2014

TABLE OF CONTENTS

Chapter 1 — Welcome	3
Introducing WWPass Security for VPN (OpenVPN)	4
Presenting Your PassKey to Your Computer	4
Related Documentation	5
Need Assistance?	6
Report a Problem from Dashboard	6
Chapter 2 — Requirements	7
Supported Platforms and Browsers	8
Chapter 3 — Setup	9
Smart Start for Setup	10
Import a Certificate for Use with Your PassKey	11
Configure the OpenVPN Client	12
Chapter 4 — Using a PassKey	14
Use a PassKey to Log Into OpenVPN on Windows	15
Use a PassKey to Log Into OpenVPN on Linux	16

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 \(OpenVPN\)](#)
- [Presenting Your PassKey to Your Computer](#)
- [Related Documentation](#)
- [Need Assistance?](#)

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.

Click [here](#) for information about PassKeys in KeySet help.



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. Click [here](#) to see a list of all documentation for the Security Pack.

Presenting Your PassKey to Your Computer

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

How do you "present" a Key to a computer? This depends on your KeySet type:

- If you have an NFC / USB KeySet, you can place a Key on an NFC reader or insert a Key into a USB Port.
- If you have a USB KeySet, you can insert a Key into a USB port.

Enter the access code for a Key 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 wrong access code three times in row, your PassKey is locked for 15 minutes and cannot be used.

Related Documentation

This documentation provides information on WWPass Security for VPN (OpenVPN) for end users.

For information on the Security Pack it is part of, click links in the list below. The list includes documentation on installing the Security Pack, on other WWPass solutions in the Security Pack, and on the WWPass KeySets that are used with these solutions for secure authentication.

WWPass KeySets and Key Services	HTML	PDF
WWPass Security Pack		
Installation		
Windows	HTML	PDF
Mac	HTML	PDF
Linux	HTML	PDF
WWPass Dashboard for Security Pack	HTML	PDF
WWPass Solutions for Security Pack		
WWPass Security for Email (Outlook & OWA)	HTML	PDF
Security for Email (Thunderbird)	HTML	PDF
WWPass Security for VPN (Juniper VPN)	HTML	PDF
Security for VPN (OpenVPN)	HTML	Currently open
WWPass Security for Windows Logon	HTML	PDF
WWPass Security for SharePoint	HTML	PDF
Personal Secure Storage		
Windows		PDF
Mac		PDF
Linux		PDF

Need Assistance?

If you encounter a problem or have a question, you can contact WWPass Product Support as follows:

Phone 1-888-WWPASS0 (+1-888-997-2770)

Email support@wwpass.com

Report a Problem from Dashboard



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

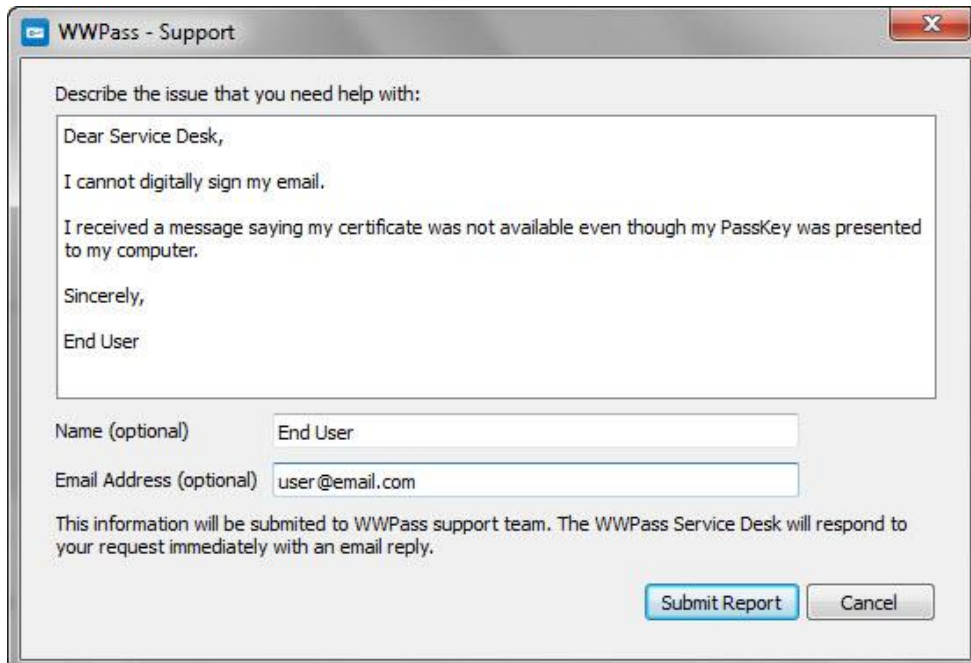
The email identifies version numbers for your Security Pack and operating system. In addition, current logs for WWPass software are automatically attached to the email.

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 ProgramData. On Linux, logs are located in HOME. Logs should not be changed before they are sent to Product Support.

To report a problem from Dashboard

1. Click the mail button  in the upper-right corner of Dashboard.
2. In the Support window that opens, type a description of the problem you need help with. You can also type a question.
3. Enter the email address Product Support should reply to. Also enter your name.
4. Click  to send your report along with the current version of all available logs.



The screenshot shows a dialog box titled "WWPass - Support". It contains a text area for describing the issue, two input fields for "Name (optional)" and "Email Address (optional)", and two buttons: "Submit Report" and "Cancel".

Describe the issue that you need help with:

Dear Service Desk,
I cannot digitally sign my email.
I received a message saying my certificate was not available even though my PassKey was presented to my computer.

Sincerely,
End User

Name (optional)

Email Address (optional)

This information will be submitted 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	<p>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:</p> <ul style="list-style-type: none">To install OpenVPN for Windows, download and run the OpenVPN installer: http://openvpn.net/index.php/open-source/downloads.htmlTo install OpenVPN for Linux (Ubuntu), run this command: <code>sudo apt-get install openvpn</code> <p>The OpenVPN client is installed on your computer and needs access to an OpenVPN server.</p>
Personal certificate for OpenVPN	<p>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.</p>
Certificate Authority (CA) certificate	<p>This is a "root" certificate that verifies your personal certificate for OpenVPN. Contact a system administrator to obtain a CA certificate and store the certificate on your computer:</p> <ul style="list-style-type: none">On Windows, you might want to store the certificate in a folder called "certs" under your OpenVPN folder.On Linux use: <code>/etc/ssl/certs/</code>
WWPass KeySet	<p>This includes the PassKey used for authentication when you log in to OpenVPN. Click here to open KeySet help.</p>
WWPass Security Pack	<p>This allows you to activate a KeySet and use WWPass Security for VPN (OpenVPN). Click the link for your operating system to open Security Pack help:</p> <ul style="list-style-type: none">WindowsLinux

Supported Platforms and Browsers

The following platforms and web browsers are supported for WWPass Security for VPN (OpenVPN). They are also supported for WWPass KeySets and Key Services. (The Mac is supported for KeySets, Key Services, and other solutions in the WWPass Security Pack.)

Requirement	Windows	Linux
<p>Operating System</p> <p><i>Outbound TCP connections must be allowed to ports 80 (HTTP) and 443 (HTTPS)</i></p>	<ul style="list-style-type: none"> • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 8 (32-bit and 64-bit) • Microsoft Windows 7 (32-bit and 64-bit) 	<ul style="list-style-type: none"> • Linux Ubuntu 12.04 LTS
<p>Web Browser</p> <p><i>For PassKey authentication and KeySet activation via WWPass Key Services</i></p>	<ul style="list-style-type: none"> • Internet Explorer 8 and later* (32-bit and 64-bit) • Chrome 20 and later • Firefox 14 and later* • Opera 11 and later 	<ul style="list-style-type: none"> • Chrome 20 through 34 • Firefox 14 and later* • Opera 11 and later (Gnome only)

* Can be used for downloading certificates from a Certificate Authority.

CHAPTER 3 — SETUP

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

Topics in this Chapter

- [Smart Start for Setup](#)
- [Import a Certificate for Use with Your PassKey](#)
- [Configure the OpenVPN Client](#)

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 the link for your operating system to open Security Pack help:
 - [Windows](#)
 - [Linux](#)
2. Obtain and activate your KeySet. Click [here](#) for KeySet help. (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 Windows, use Firefox or Internet Explorer
 - On Linux, use Firefox

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 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. [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 included in the 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:

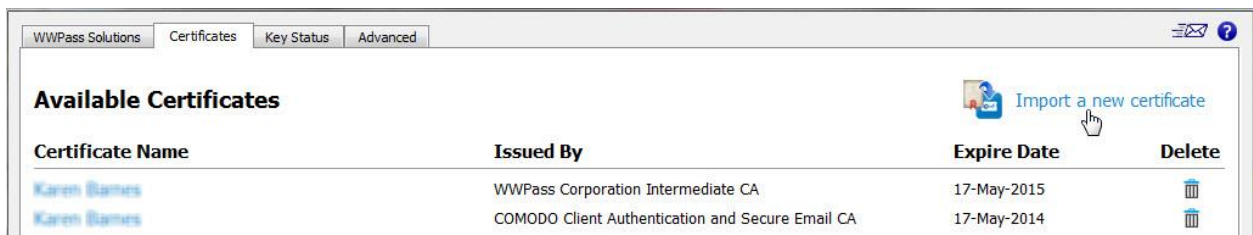
- Remove the certificate file from your computer. At this point, the certificate is securely stored in WWPass cloud storage, where it is encrypted, fragmented, and dispersed.


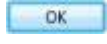



Note: See the [Smart Start](#) for a list of all steps in the setup process.

To import a certificate

1. Present your PassKey to your computer.
2. Open the WWPass Dashboard using its Key icon .
3. From the Certificates tab, click **Import a new certificate** .



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

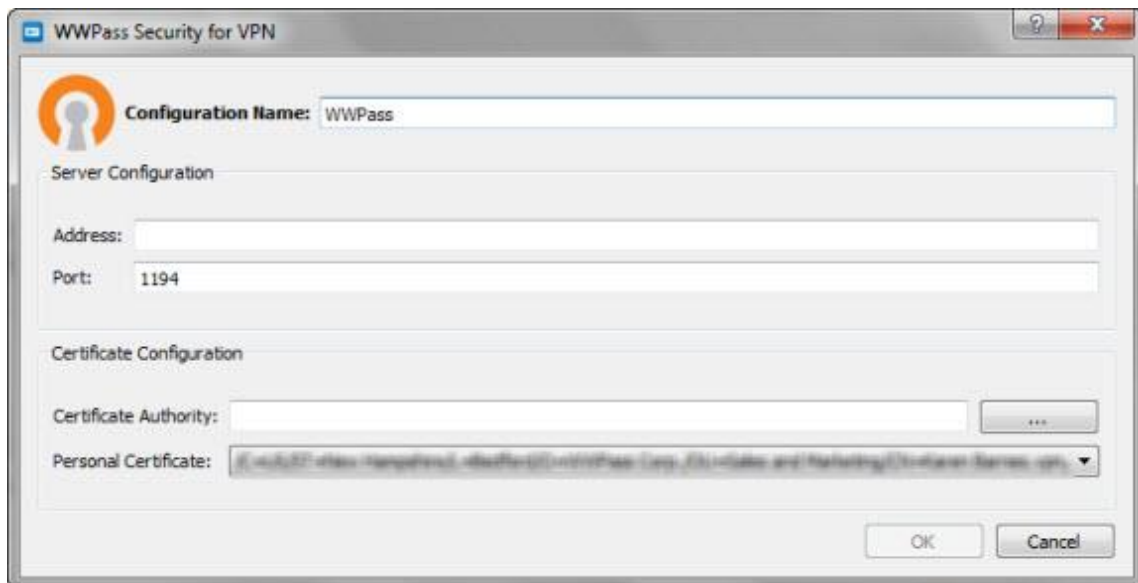
1. [Present](#) your PassKey to your computer.
2. Open the WWPass Dashboard using its Key icon .
3. From the WWPass Solutions tab, click **Configure OpenVPN** next to WWPass Security for VPN. Then click from the User Account Control message.



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 .
 - **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.



5. Click in the WWPass Security for OpenVPN window. When the OpenVPN Configuration window displays the contents of the configuration file, click 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](#)
- [Use a PassKey to Log Into OpenVPN on Linux](#)

Use a PassKey to Log Into OpenVPN on Windows

Follow 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) Present your PassKey to your computer.
- 2) Right-click the system tray icon  for OpenVPN.
- 3) Select the Open VPN server to connect to (if more than one is available) and click **Connect**.
- 4) When prompted, enter your PassKey access code and click .

To log in with your PassKey from the Windows Command Prompt

1. Present 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. Present your PassKey to your computer.
2. Start OpenVPN with this 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.

