USER GUIDE

WWPass Dashboard

For WWPass Security Pack 3.2

May 2015

TABLE OF CONTENTS

Chapter 1 — Welcome 4
Introducing the WWPass Dashboard 5
Tabs in Dashboard 6
Connecting Your PassKey/PassKey for Mobile to Your Computer 6
Related Documentation 7
Need Assistance? 8
Report a Problem from Dashboard 8
Chapter 2 — Requirements 10
Chapter 3 — The Basics 11
Start Dashboard 12
Use the Key Icon for Dashboard 15
Exit from Dashboard 16
Chapter 4 — WWPASS Solutions Tab 18
Overview for the WWPass Solutions Tab 19
Solutions available for Windows 19
Solutions available for Mac 20
Solutions available for Linux 21
Secure by WWPass 22
Personal Secure Storage 22
BlackBook 22
Features for BlackBook 23
Secure with WWPass 24
Features for Firefox 25
Features for Thunderbird 26
How to configure OpenVPN 27
How to Secure 28
Chapter 5 — Certificates Tab 29
Overview for the Certificates Tab 30
About Certificates 31
Using the Certificates tab 32
View Certificate Details 32
Information in Certificate Details 33
Check Expiration Date for a Certificate 34
Import a certificate 34
Delete a Certificate 37
Chapter 6 — Key Status Tab 38
Overview for the Key Status Tab 39

Using the Key Status tab 40
Status Reference Chart 41
Chapter 7 — Advanced Tab 43
Overview for the Advanced Tab 44
Using the Enable SSL Encryption Feature 44
Using the HTTP Proxy Feature 45
Using the Smart Card Removal Feature 46
Using the WWPass Credential Provider Feature 47
Using the Mobile Key Pairing 49
Chapter 8 — Update the Security Pack 52
Overview for Updating the WWPass Security Pack 53
Steps to follow 53
How to tell if an update is needed 53
Update the WWPass Security Pack on Windows 54
Update the Security Pack on a Mac 55
Update the Security Pack on Linux 56

CHAPTER 1 — WELCOME

This chapter introduces the WWPass® Dashboard™. It also provides information on using a PassKey™ and a PassKey for Mobile from WWPass, accessing related documentation, and contacting WWPass Product Support.

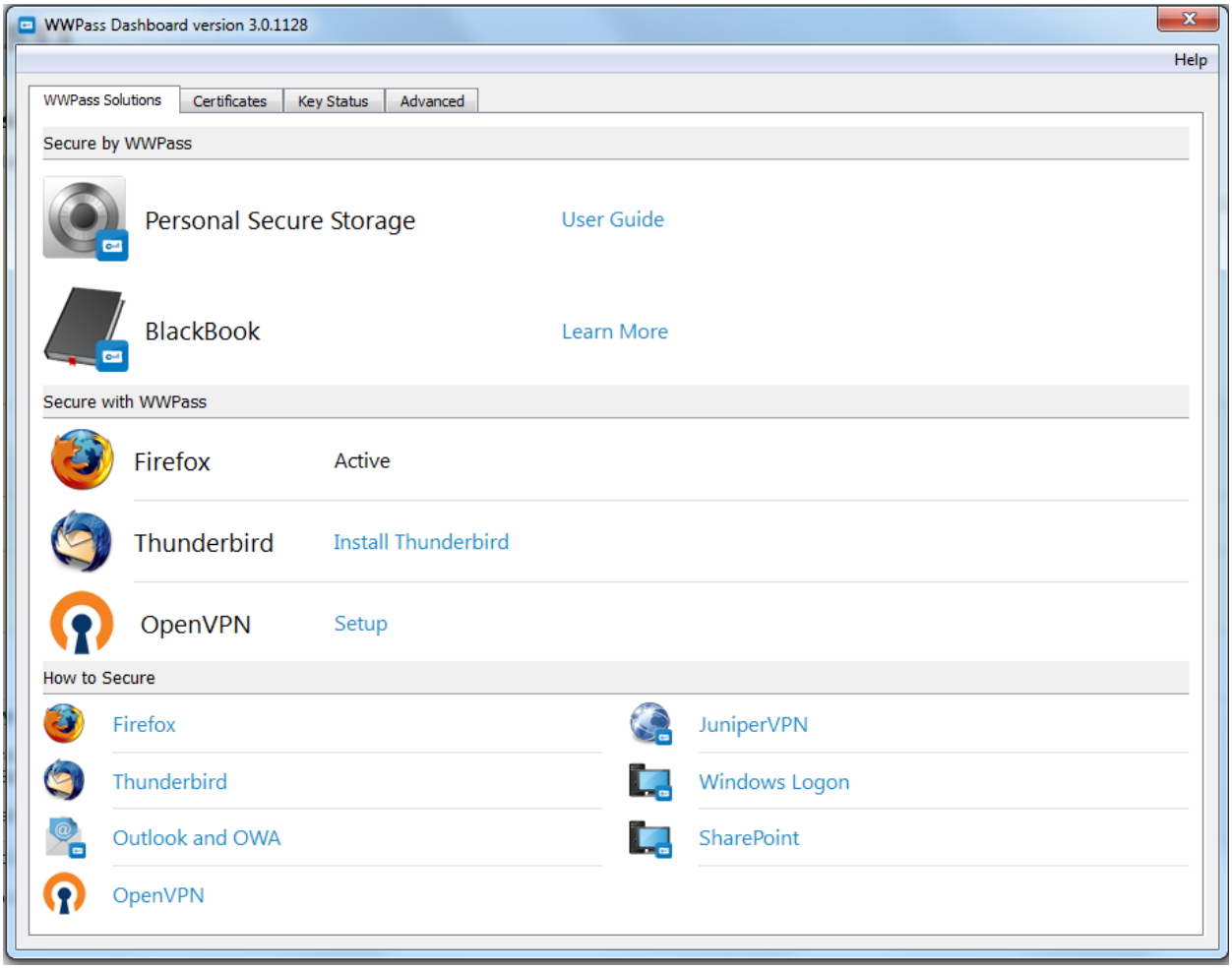
Topics In This Chapter

- Introducing the WWPass Dashboard
- Connecting Your PassKey or PassKey for Mobile to Your Computer
- Related Documentation
- Need Assistance?

Introducing the WWPass Dashboard

This documentation covers using the WWPass Dashboard on Windows, Mac, and Ubuntu 12.04 Precise Pangolin and Ubuntu 14.04 Trusty Tahr.

Dashboard is included in the WWPass Security Pack™, the software pack that allows you to activate a PassKey or a PassKey for Mobile and use it to prove your identity with WWPass authentication solutions.



Dashboard provides a "control panel" with four tabs that let you:

- See which WWPass solutions are part of the Security Pack for your operating system.
- Open documentation for WWPass solutions.
- Configure several WWPass solutions.
- Check the status of your soft token (WWPass Passkey for Mobile application on your smartpone) or of the Keys in your WWPass KeySet, which includes the hardware PassKey used for authentication.
- View all certificates associated with your PassKey or PassKey for Mobile, import certificates and delete certificates.
- Specify advanced settings for SSL encryption and more.

- Pair your smartphone with Mobile Key to your computer to begin using it as a PassKey.
- Email a question or problem to WWPass Product Support.

When a new version of the Security Pack is available, this is indicated in Dashboard on Windows and Mac. You can use features in Dashboard to update the Security Pack on both platforms.

Tabs in Dashboard

Click links below to see information on each tab in Dashboard:

- WWPass Solutions
- Certificates
- Key Status
- Advanced

Connecting Your PassKey/PassKey for Mobile to Your Computer

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

How do you "connect" 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 connect a Key to a USB Port.
- If you have a USB KeySet, you can connect a Key to a USB port.
- If you have a PassKey for Mobile application, you can pair it with your computer.

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 a row, your PassKey is locked for 15 minutes and cannot be used.

Related Documentation

Here is a list of all documentation for WWPass Dashboard and the WWPass Security Pack (which includes Dashboard). The list includes documentation on installing the Security Pack, on 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 PassKey for Mobile (Android)	HTML	PDF

WWPass Security Pack		
Installation		
Windows	HTML	PDF
Mac	HTML	PDF
Linux	HTML	PDF
WWPass Dashboard for Security Pack	HTML	Currently open
WWPass Solutions for Security Pack		
WWPass Security for Firefox		PDF
WWPass BlackBook	HTML	
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	PDF
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.

The email automatically identifies version numbers for the WWPass Security Pack and your operating system. In addition, the current versions of logs for all 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.

Logs are located:

on Windows:

System log: C:\ProgramData\WWPass\wwpass-s.log
User log: %HOME%\AppData\Local\WWPass\wwpass.log

on Mac:

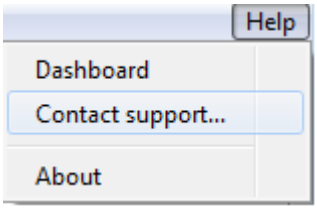
System log: /var/log/wwpass/wwpass-s.log
User log: $HOME/Library/Logs/wwpass/wwpass.log

on Linux:

System log: /var/log/wwpass/wwpass-s.log
User log: $HOME/.cache/wwpass/wwpass.log

To report a problem from Dashboard

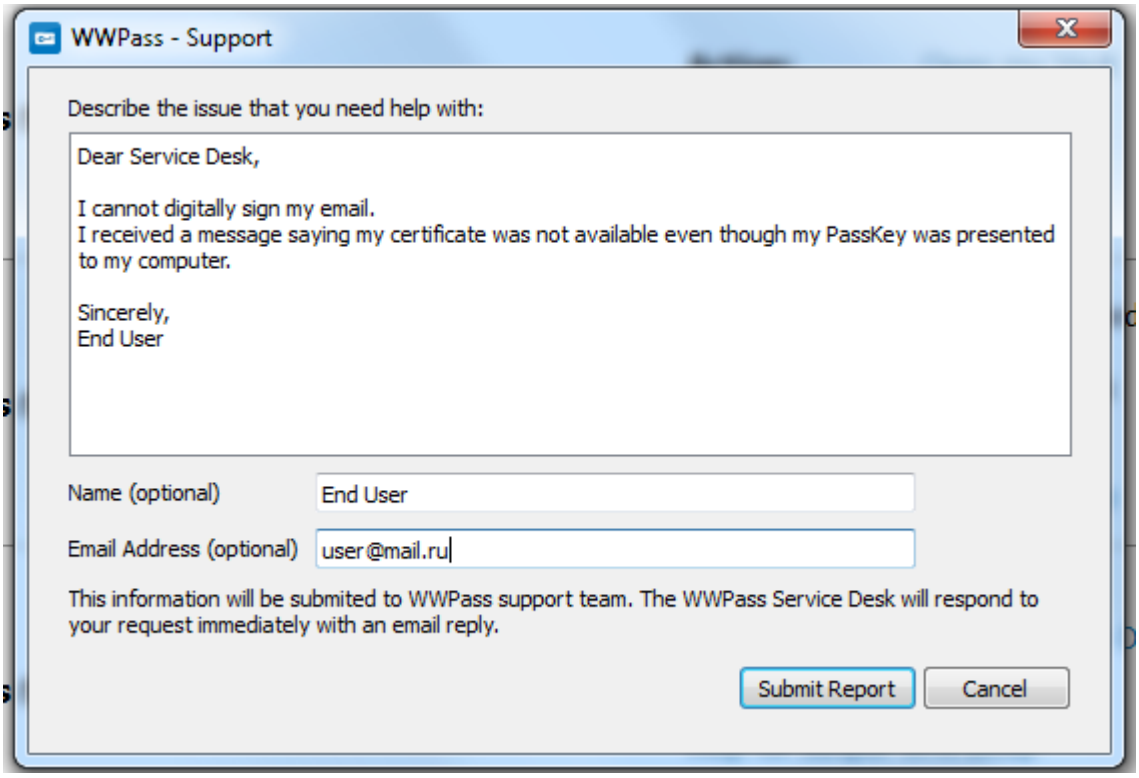
1. Click **Help** in the upper-right corner of Dashboard and then **Contact support** as shown below.



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.



CHAPTER 2 — REQUIREMENTS

Below are platform and browser requirements for the WWPass Dashboard. These are the same as requirements for the WWPass Security Pack, which includes Dashboard. Additional requirements for solutions in the Security Pack are covered in the documentation for each solution.

Requirement	Windows	Mac	Linux
Operating System	• 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)	• Mac OS X 10.8 and later	• Ubuntu 14.04 LTS (Trusty Tahr) • Ubuntu 12.04 LTS (Precise Pangolin)
Web Browser *For PassKey use and KeySet activation via WWPass Key Services*	• Internet Explorer 8 and later* (32-bit and 64-bit) • Chrome 20 and later • Firefox 14 and later* • Opera 11 and later	• Safari 5 and later • Chrome 20 and later • Firefox 14 and later*	• Firefox 14 and later* • Opera 11 and later (Gnome only)

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

CHAPTER 3 — THE BASICS

This chapter covers starting and exiting from WWPass Dashboard.

Topics In This Chapter

- Start Dashboard
- Exit from Dashboard
- Use the Key Icon for Dashboard

Start Dashboard

This topic tells you how to start and open the WWPass Dashboard on:

- Windows
- Mac
- Linux

When you start Dashboard, its key icon is added to the system tray (Windows), the menu bar (Mac), or the notification area (Linux).

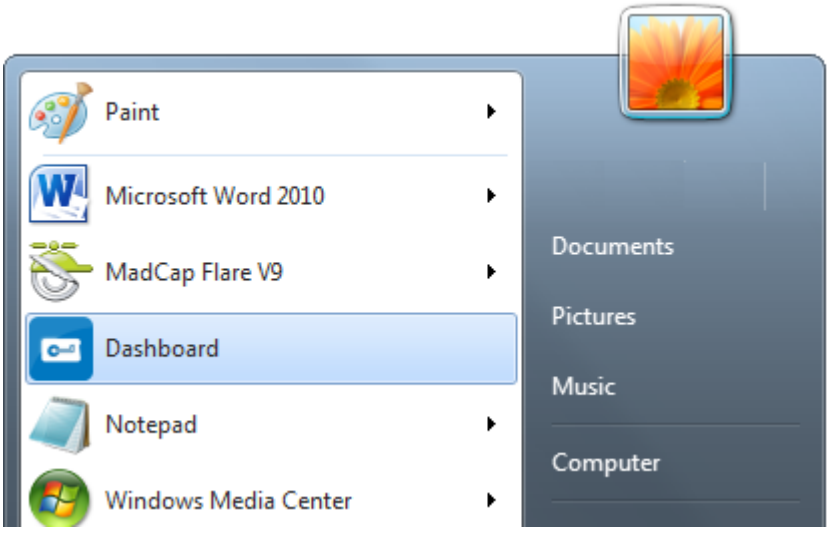
You can use the key icon to open Dashboard. You can also use the key icon to see whether your PassKey or PassKey for Mobile is connected to your computer (it must be connectted before you can view Dashboard's Certificates tab and Key Status tab). Click here to see the different ways the icon is shown.

Once Dashboard is started, it continues running and the key icon remains available. Dashboard only stops running when you exit. Closing Dashboard does not stop it or clear the key icon.

Once Dashboard is open, you can display any of the tabs it contains by clicking the tab.

To start Dashboard on Windows

1. Start Dashboard from the Windows Start Menu. The Dashboard icon is added to the system tray.



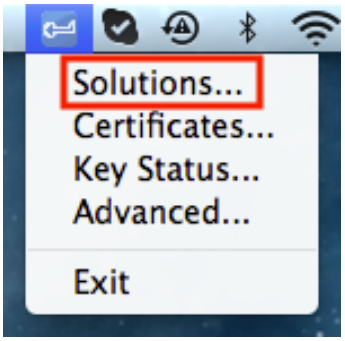
2. Open Dashboard by clicking its icon in the system tray. Dashboard opens to the tab that was selected the last time it was used. To select which tab to display, right-click the key icon and click on the tab in the menu that appears.


Solutions...
Certificates...
Key Status...
Advanced...
Exit
Customize...

To start Dashboard on Mac

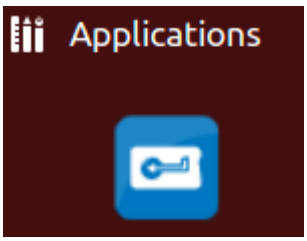
1. Start Dashboard from Applications in Finder. Its key icon is added to the menu bar. (Skip this step if the key icon is already shown in the menu bar.)

2. Open Dashboard by clicking its key icon in the menu bar and selecting a tab. Dashboard opens to the selected tab.

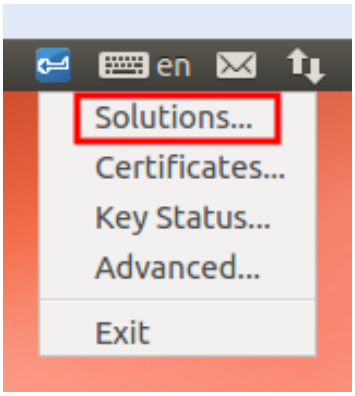


To start Dashboard on Linux

1. Launch Dashboard from Applications.



2. Open Dashboard by clicking its key icon in the notification area. Dashboard opens to the tab that was selected the last time it was used. To select which tab to display, right-click the key icon and click on the tab in the menu that appears.



Use the Key Icon for Dashboard

When you start Dashboard, its key icon is added to the system tray (Windows), the menu bar (Mac), or the notification area (Linux).

The key icon lets you open Dashboard and is displayed in different ways to let you see the following at a glance:

The Key icon is blue when your PassKey is connected to your computer. It must be connected before you can view Dashboard's Certificates tab and Key Status tab.

The Key icon is gray when your PassKey is not connected to your computer.

The Key icon is yellow when an NFC reader is available but a PassKey is not connected to your computer.

The Key icon is red when the Windows Smart Card service (SCardSvr) is not running. PassKeys use Smart Card technology.

The Key icon is shown with an exclamation point when:

- A new version of the WWPass Security Pack is available.
- The computer needs to be restarted after installation or after an update of the WWPass Security Pack. A restart enables all features of the Security Pack.

Exit from Dashboard

This topic tells you how to close and exit from the WWPass Dashboard:

- Closing Dashboard clears it from your desktop. However, it continues running as a process and its key icon remains available so that you can quickly open Dashboard.
- Exiting from Dashboard stops it from running.

Close Dashboard

To close Dashboard on any operating system, click the **X** button at the top of Dashboard

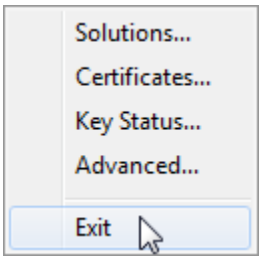
Windows **X** button

Mac **X** button

Linux **X** button

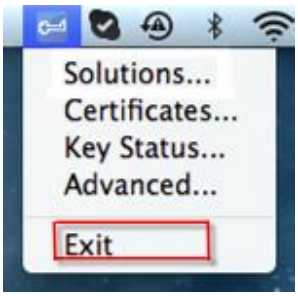
To exit from Dashboard on Windows

1. Right click Dashboard's Key icon in the system tray.
2. Click **Exit** in the menu that appears.



To exit from Dashboard on Mac

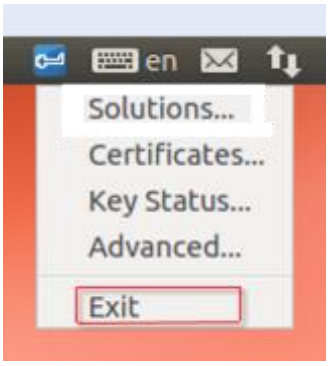
1. Click Dashboard's key icon in the menu bar.
2. Click **Exit** in the menu that appears.



To exit from Dashboard on Linux

1. Right-click Dashboard's key icon in the notification area.

2. Click **Exit** in the menu that appears.



CHAPTER 4 — WWPASS SOLUTIONS TAB

This chapter covers using the WWPass Solutions tab in the WWPass Dashboard.

Topics In This Chapter

- Overview
- Secure by WWPass
- Secure with WWPass
- How to secure

Overview for the WWPass Solutions Tab

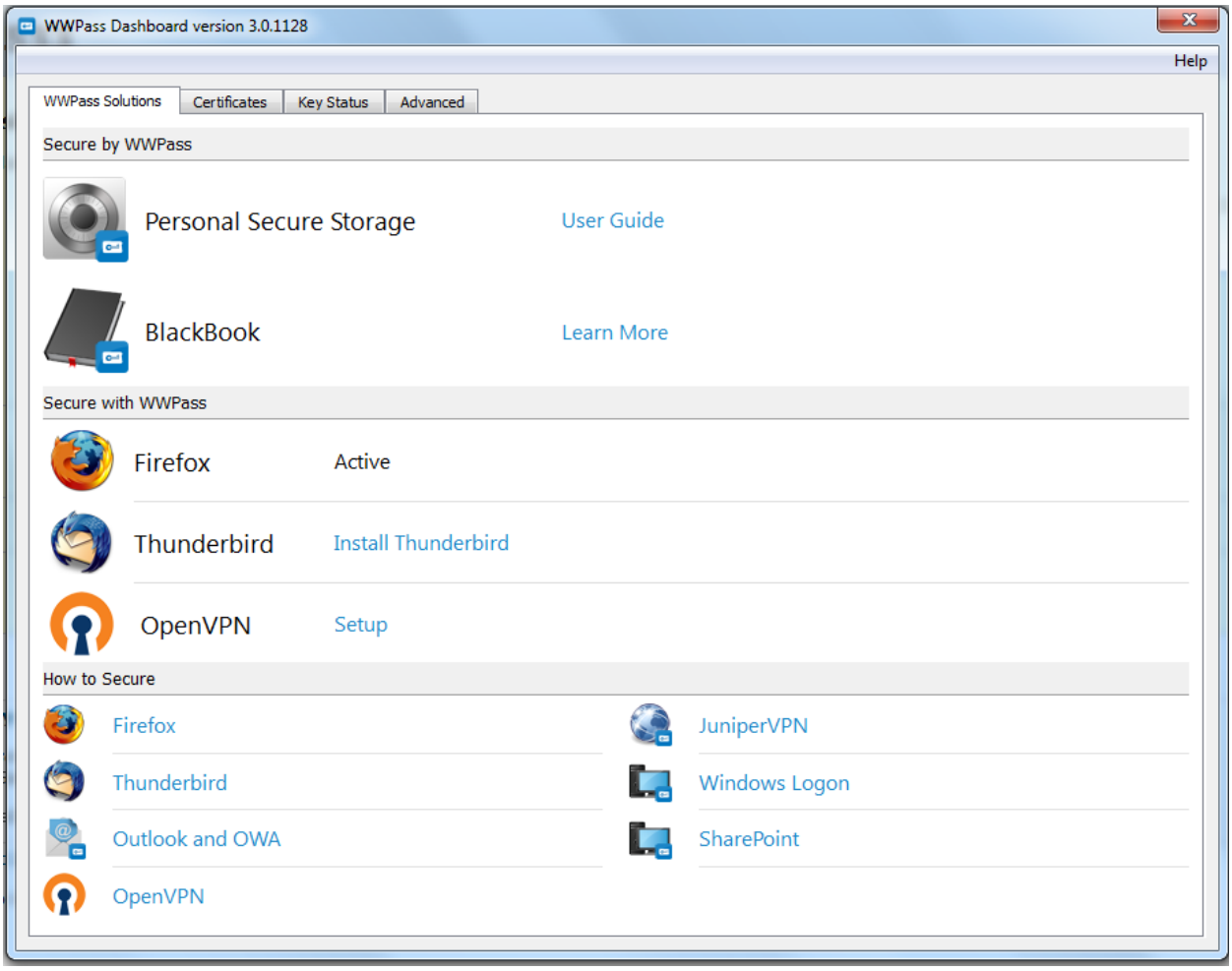
The WWPass Solutions tab shows the WWPass solutions included in the WWPass Security Pack. It also shows the status and version number for this software pack, and lets you update the Security Pack.

Solutions are grouped by type—Secure by WWPass (Personal Secure Storage and BlackBook), Secure with WWPass and How to Secure. Click the links below for information on each group:

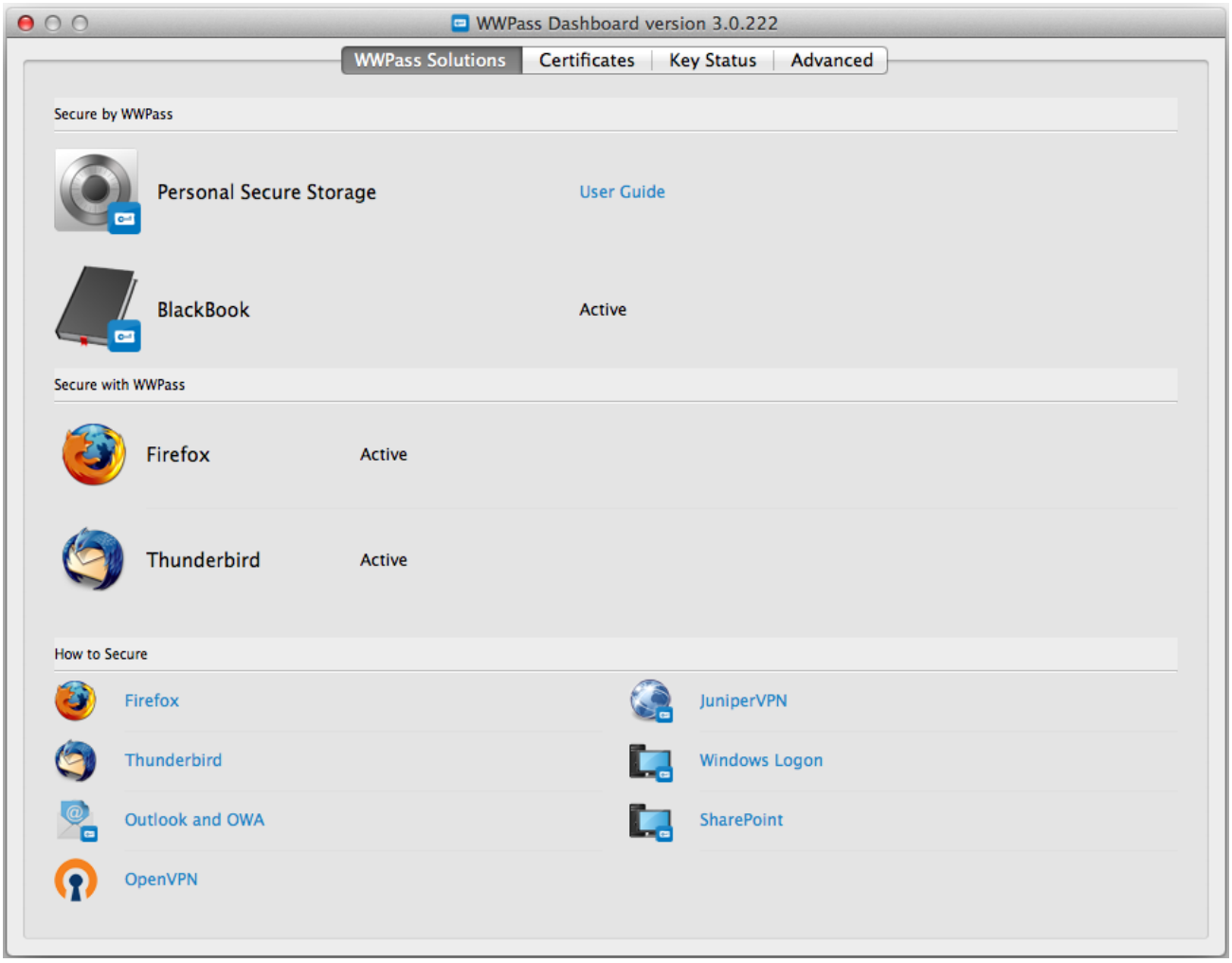
- Secure by WWPass
- Secure with WWPass
- How to Secure

Which solutions are available in the WWPass Solutions tab depends on whether your operating system is Windows, Mac or Linux.

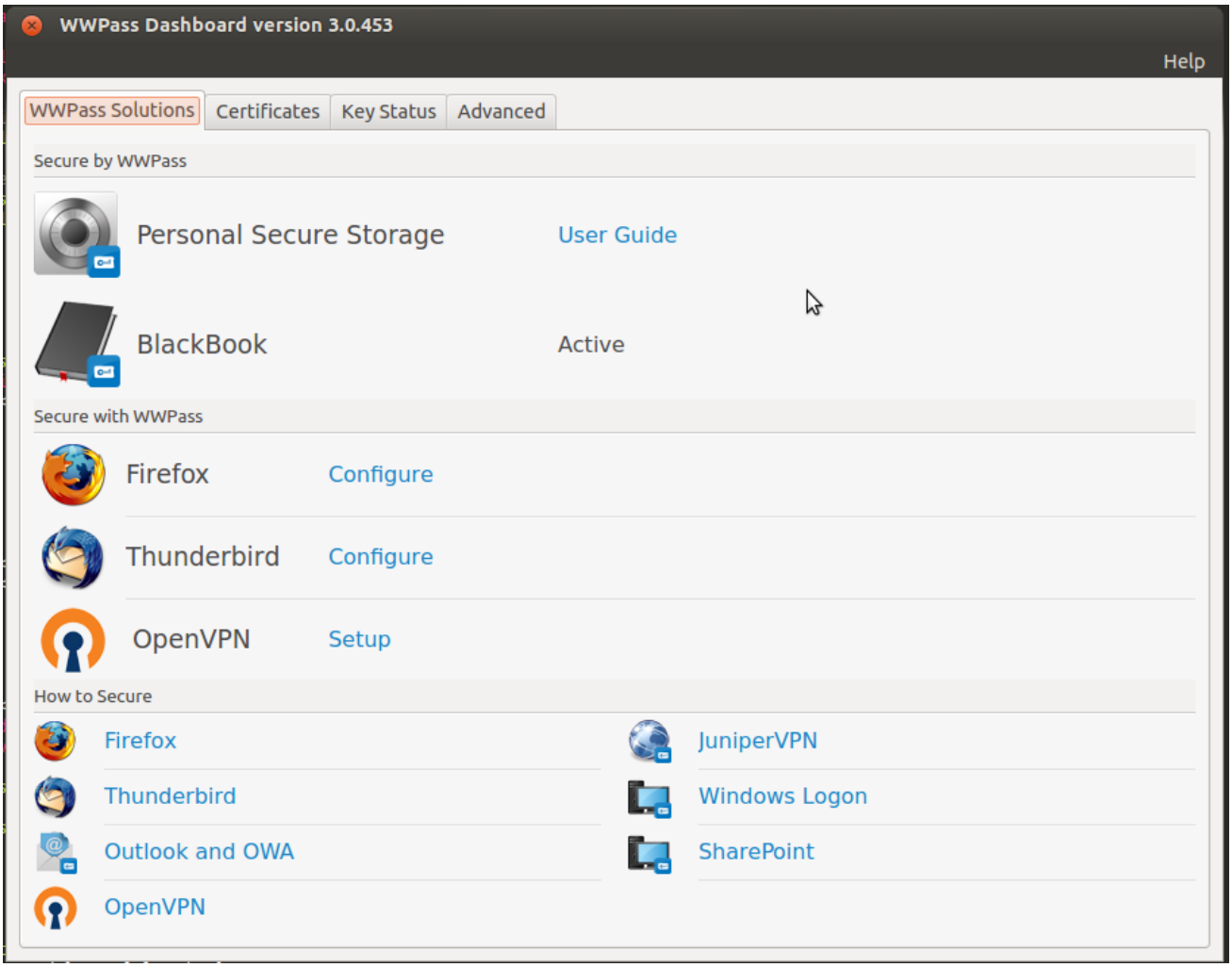
Solutions available for Windows



Solutions available for Mac



Solutions available for Linux



Secure by WWPass

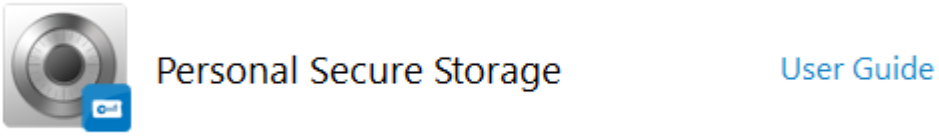
Secure by WWPass group includes WWPass software applications.

Personal Secure Storage

This lets you run WWPass Personal Secure Storage (PSS).

PSS allows you to store confidential files in your personal vault in the WWPass cloud. Your data is encrypted, fragmented and dispersed in WWPass data centers around the globe so that it cannot be stolen. Only you can access files stored in PSS using your PassKey or PassKey for Mobile.

Running PSS is described below. To open PSS documentation, click the **User Guide** link shown in Dashboard.



To start PSS and open your vault

1. Connect your PassKey or PassKey for Mobile to your computer.
2. Click Dashboard's WWPass Solutions tab.
3. Click the PSS icon in the Personal Secure Storage.
4. Enter the access code for your PassKey/PassKey for Mobile, when prompted. PSS opens and your personal vault is displayed.

BlackBook

This solution securely stores your website credentials and automatically enters them when you need to log in.

BlackBook remembers your usernames and passwords so that you don't have to. It is more secure than other password managers because it does not store your credentials locally. Instead, it encrypts and fragments credentials and distributes them in WWPass cloud storage centers around the globe. Each fragment is in a different location so there is no single point of vulnerability. When you log into a website with BlackBook, it reads your PassKey or PassKey for Mobile to gather your credentials from the cloud and automatically enter them for you. Click here for information on Dashboard features for BlackBook. Click here for BlackBook help.

Features for BlackBook

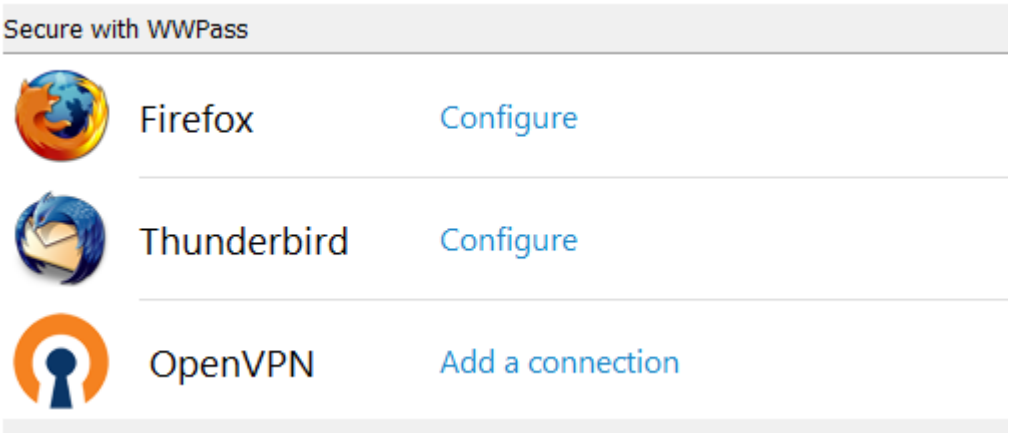
Dashboard features for BlackBook let you check its setup status and install the software as an add-on in Firefox and in Chrome. Be sure to install Firefox before you install BlackBook.

Status	What It Means	What To Do
Learn More: BlackBook	Shown when BlackBook is not installed in either Firefox or Chrome.	Install BlackBook: 1. Click the **Learn More** link next to BlackBook in the WWPass Solutions tab. The BlackBook page on the WWPass website opens in the Firefox or Chrome web browser. 2. From the BlackBook page, click the **Download** button. 3. Click **Allow** in the message that says "Firefox/Chrome prevented this site from asking you to install software on this computer". 4. Click **Install Now** in the software installation window that opens. When installation is complete, the "installed successfully" message appears, BlackBook controls are added to the Firefox/Chrome navigation bar, and you are prompted to connect your PassKey/PassKey for Mobile access code to enable BlackBook.
Active: BlackBook	Shown when BlackBook is installed in Firefox and Chrome.	Use it to securely store and enter your website credentials.
Active in Firefox, available for Chrome	Shown when BlackBook is installed in Firefox but not installed in Chrome, when Chrome is available.	Optionally enable BlackBook in Chrome and use it to securely store and enter your website credentials in either web browser.
Active in Chrome, available for Firefox	Shown when BlackBook is installed in Chrome but not installed in Firefox, when Firefox is available.	Optionally enable BlackBook in Firefox and use it to securely store and enter your website credentials in either web browser.

Secure with WWPass

You can use solutions and features in the Secure with WWPass group to securely exchange encrypted and digitally signed email, securely log into your VPN (virtual private network). The group includes:

- **Mozilla Firefox**—Firefox is one of two web browsers you can use to download an email certificate for authentication with a PassKey or PassKey for Mobile. Firefox can be used on Windows, Mac, and Linux. Internet Explorer can be used on Windows. Email certificates prove your identity. They can be downloaded from a third-party Certificate Authority (CA) such as Comodo. Click here for information on Dashboard features for Firefox.
- **Thunderbird**—This solution allows you to authenticate with a PassKey or PassKey for Mobile when you exchange digitally-signed or encrypted email in Mozilla Thunderbird. Click here for information on Dashboard features for Thunderbird.
- **OpenVPN** - This solution (available for Windows and Linux) allows you to log into OpenVPN using a PassKey or PassKey for Mobile instead of a username and password. You can then access all files and applications you have permissions for on your network. Dashboard features are links that let you configure the OpenVPN client (see below) and open help for WWPass Security for VPN (OpenVPN).



Features for Firefox

Dashboard features for Firefox let you check its setup status, download the browser, and configure it with WWPass software for PassKey/Passkey for Mobile authentication.

Status	What It Means	What To Do
Active: Firefox	Shown when Firefox is installed and configured.	Use Firefox to download certificates for WWPass solutions. Also use it with BlackBook to securely store and automatically enter website credentials.
Needs Setup: Set up Firefox	Shown when Firefox is not installed.	Download Firefox: 1. Click the **Set up Firefox** link in the WWPass Solutions tab. 2. Click http://www.mozilla.org/firefox in the message that appears. The Mozilla download page for Firefox appears. 3. Download Firefox from Mozilla's site. Then install the browser.
Needs Setup: Configure Firefox	Shown when Firefox is installed but not configured with WWPass software.	Load WWPass software as a security device into Firefox's Device Manager: 1. Click the **Configure Firefox** link in the WWPass Solutions tab. 2. WWPass software is loaded into Firefox and shown as a PKCS#11 module in Firefox's Device Manager window. If Firefox was open during configuration, you are prompted to restart it.

Features for Thunderbird

Dashboard features for Thunderbird let you check its setup status, install it, and configure it with WWPass software for PassKey/PassKey for Mobile authentication.

Features also include a link that lets you quickly open help for WWPass Security for Email (Thunderbird).

Status	What It Means	What To Do
Active: Thunderbird	Shown when Thunderbird is installed and configured with WWPass software.	Use WWPass Security for Email (Thunderbird) to securely send encrypted and digitally-signed email messages.
Needs Setup: Set up Thunderbird	Shown when Thunderbird is not installed.	Install Thunderbird: 1. Click the **Set up Thunderbird** link in the WWPass Solutions tab. 2. Click http://www.mozilla.org/thunderbird in the message that appears. The Mozilla download page for Thunderbird appears. 3. Download Thunderbird from Mozilla's site and install the browser.
Needs Setup: Configure Thunderbird	Shown when Thunderbird is installed but not configured with WWPass software.	Load WWPass software as a security device into Thunderbird's Device Manager: 1. Click the **Configure Thunderbird** link in the WWPass Solutions tab. 2. WWPass software is loaded into Thunderbird. WWPass PassKey/PassKey for Mobile is then shown in Thunderbird's Device Manager window. If Thunderbird was open during configuration, you are prompted to restart it.

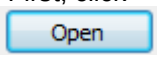
How to configure OpenVPN

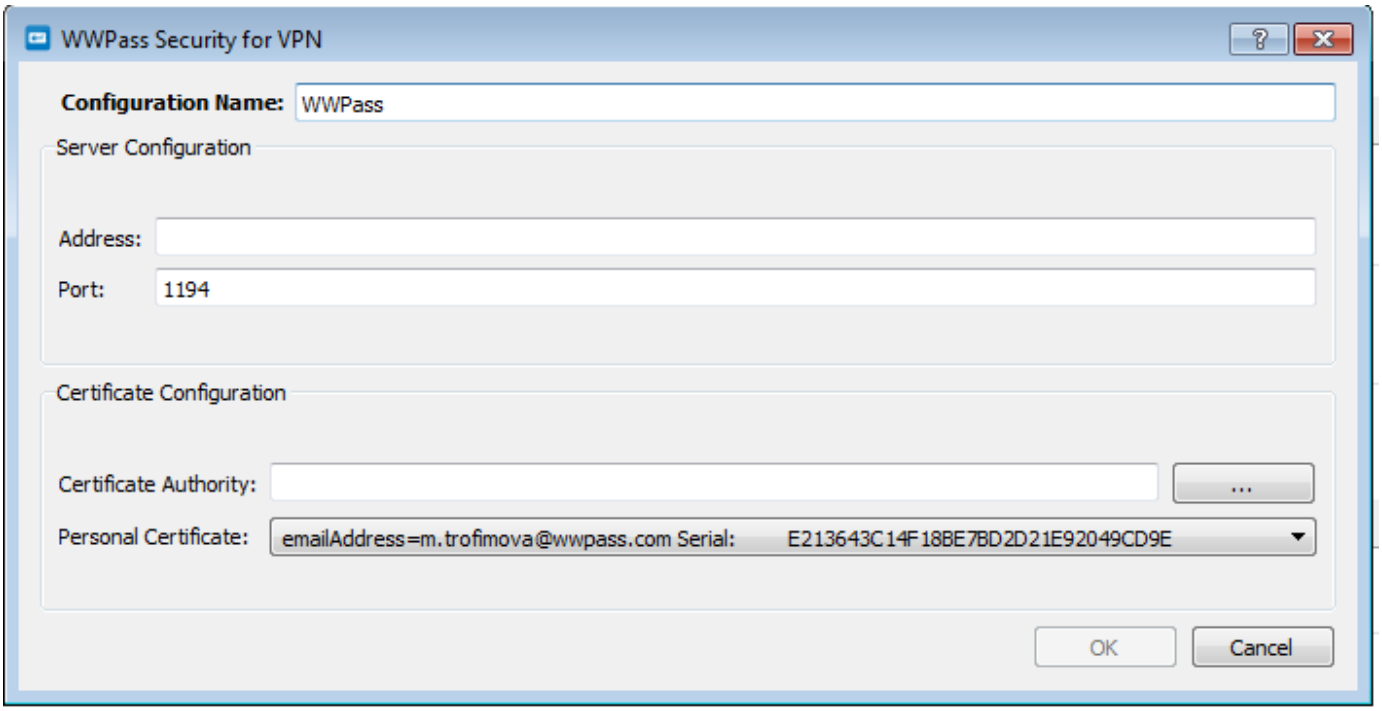
Follow the steps below to configure the OpenVPN client for authentication with your PassKey or Passkey for Mobile. These steps create a configuration file that is associated with your PassKey/PassKey for Mobile and OpenVPN certificate. If multiple users run OpenVPN from the same computer, each user needs their own configuration file on that computer. Configuration files are automatically stored in the OpenVPN folder.

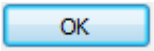
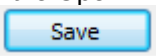
Before you begin:

- Obtain a personal certificate for OpenVPN and associate it with your PassKey or PassKey for Mobile. 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 or PassKey for Mobile.
- Also obtain a Certificate Authority certificate for OpenVPN, create a "certs" folder under your OpenVPN folder and save the Certificate Authority certificate in "certs".

To configure the OpenVPN client

1. Connect your PassKey or PassKey for Mobile to your computer.
2. Click Dashboard's WWPass Solutions tab.
3. Click **Add a connection** in the OpenVPN in the Secure with WWPass group.
4. From the WWPass Security for OpenVPN window, enter or selsct configuration settings as follows:
   - **Configuration Name:** Enter the name to use for the OpenVPN 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 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 certificate for OpenVPN. First, click  . Then select the certificate file 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 displys 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.

How to Secure

How to secure group provides you with links to Help Guides on using WWPass with third-party software:

- Firefox
- Thunderbird
- Outlook and OWA
- OpenVPN
- JuniperVPN
- Windows Logon
- Sharepoint

CHAPTER 5 — CERTIFICATES TAB

This chapter covers using the Certificates tab in the WWPass Dashboard.

Topics In This Chapter

- Overview
- Using the Certificates Tab
- About Certificates
- View Certificate Details
- Check Expiration Date for a Certificate
- Import a Certificate
- Delete a Certificate

Overview for the Certificates Tab

The Certificates tab displays a list of all X.509 certificates associated with your PassKey or PassKey for Mobile.

- Manage the certificates that are associated with your WWPass PassKey/Passkey for Mobile and used for authenticating your identity with WWPass solutions. Features for certificates can be used to:
  - View all certificates associated with a PassKey/Passkey for Mobile.
  - Import certificates for use with a PassKey/PassKey for Mobile.
  - Delete certificates that are no longer needed.

The certificates prove your identity when you use your PassKey or PassKey for Mobile to authenticate with a domain, application, service, or website.

The following information is shown for each certificate:

- **Certificate Name**—This is a certificate's common name. It might be your name or a long alpha-numeric text string.
- **Issued By**—This is the Certificate Authority (CA) that issued a certificate.
- **Expire Date**—This is the date a certificate will expire. Click here to learn more about expiration date.

To view additional information about a certificate, click its name in the Certificates tab. The Certificate Details window opens. From Certificate Details, you can open a Windows operating system window with system information on the certificate.

About Certificates

Certificates are obtained from a trusted Certificate Authority (CA). This can be a third-party CA such as Comodo or your organization's internal CA.

Once a certificate is associated with your PassKey or PassKey for Mobile, it is stored in WWPass cloud storage, where it is encrypted, fragmented, and dispersed. There is no single point of vulnerability from which it could be stolen.

Each certificate specifies your name and certifies that the public key included in the certificate belongs to you. The public key is part of a public/private key pair that lets you use digital signing and encryption to securely and privately exchange data over a network or the Internet:

- **Public key**—This can be distributed freely and is published as part of a certificate. You can share it with others so that they can use it to encrypt the email and data they send you.

- **Private key** —This corresponds to the public key but is kept secret and is only available to you. It is used to decrypt email and data that were encrypted with your public key. Data encrypted with a public key can only be decrypted with the corresponding private key.

Note: If you download a certificate from a third-party, do this using Firefox as the web browser on Windows, Mac or Linux or Internet Explorer on Windows.

Using the Certificates tab

In order to view information in the Certificates tab, you need to connect your PassKey or Passkey for mobile to your computer. If your PassKey/PassKey for Mobile is not connected, the tab displays a message asking you to connect it. After you connect your PassKey or PassKey for Mobile, the message is replaced with certificate information.

In addition to viewing certificate information, you can use the Certificates tab to:

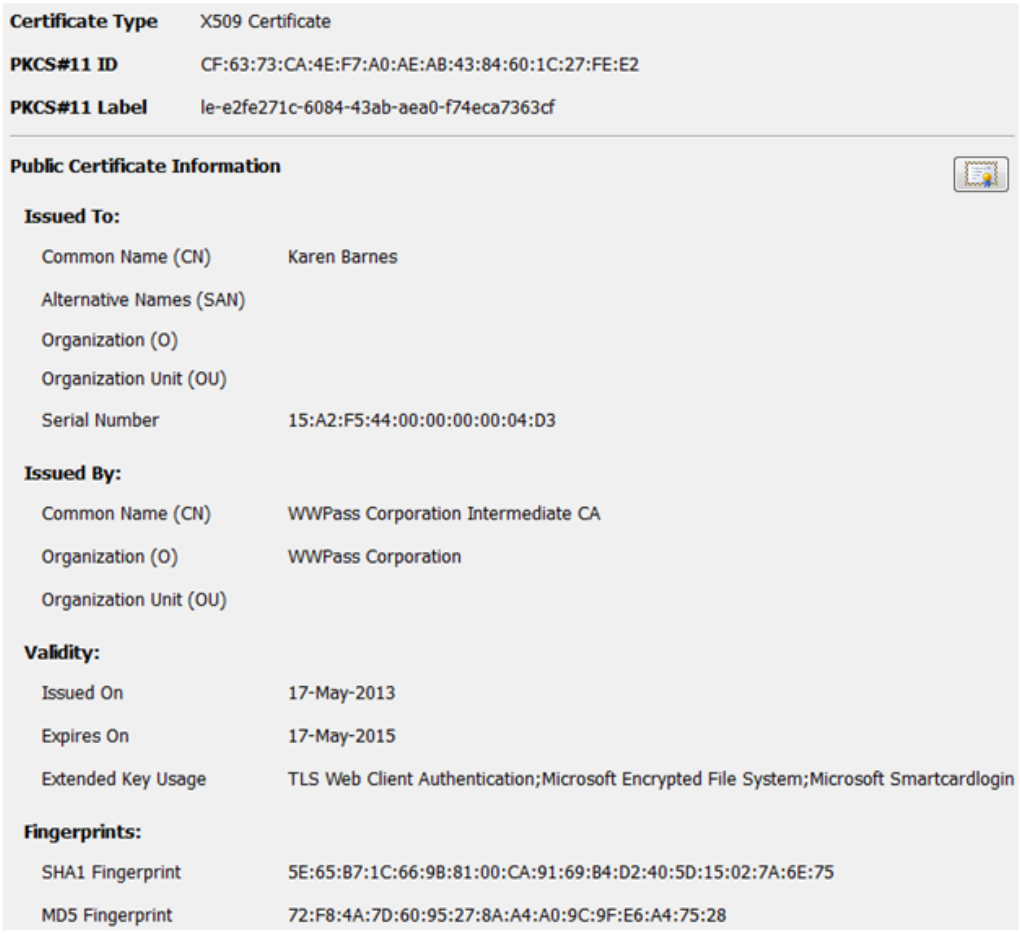
- View certificate details
- Check certificate expiration dates
- Import certificates for use with your PassKey
- Delete certificates

View Certificate Details

To view details for a certificate, click the certificate's name in Dashboard's Certificates tab.

The Certificate Details window opens with additional information, including certificate type. This is always X.509, which is a widely-used standard for defining public keys.

If you are running Dashboard on Windows and want to view system information for a certificate, click  at the top of Certificate Details. An operating system window opens with more details and information such as the certificate's purpose and certification path (chain of trust).



Information in Certificate Details

Most information in Certificate Details is for the public key included in the selected certificate. Information is presented in sections as follows:

- **Issued To:** This section shows the common and alternative names for the certificate plus the serial number that uniquely identifies it. Common name identifies the certificate owner and usually reflects their name, for example: Joe User. If the certificate is for use with an organization, this section might also show:
  - Names of the organization and the certificate owner's organizational unit. The latter can help identify the purpose of the certificate. For example, if "Corporate Secure Email" is shown, this indicates the certificate is for email authentication.
  - The **Common Name (CN)** field might show information such as the owner's username for the organization domain, for example: Joe User / j.user@organization.com.

- **Issued By:** This section shows the common name of the Certificate Authority (CA) that issued the certificate. It also shows the organization and organizational unit to which the certificate issuer belongs.

- **Validity:** This section shows the date a certificate was issued and the date it will expire. Prior to its expiration date, the certificate must be renewed or a new certificate for the same purpose must be obtained and associated with your PassKey or PassKey for Mobile. If an expired certificate is no longer needed, it can be deleted. Extended Key Usage indicates the purpose of a certificate's public key. For

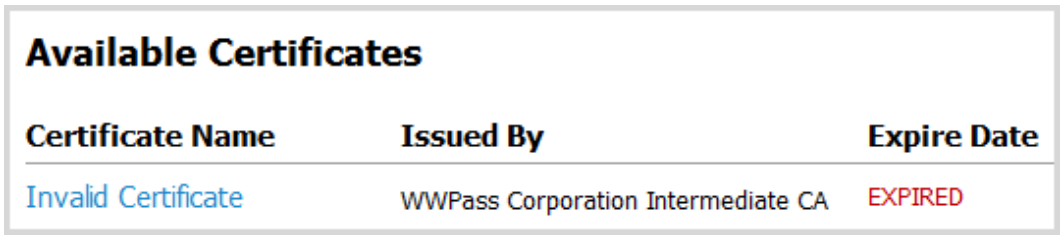
example, it might show that a certificate is used to prove your identity to a remote computer, to encrypt file data, and for Smart Card logon.

- **Fingerprints:** This section shows the unique numbers associated with a public key certificate. These can be used to verify that the certificate has not been tampered with.

Check Expiration Date for a Certificate

To see when a certificate will expire, check the **Expire Date** column in the Certificates tab:

- If a certificate is not due to expire soon, its expiration date is shown in black.
- If a certificate is due to expire in one month or less, its expiration date is shown in **red**.
- If a certificate has expired, the word "EXPIRED" replaces the expiration date and "Invalid Certificate" replaces name in the **Certificate Name** column.



Prior to its expiration date, a certificate must be renewed or a new certificate for the same purpose must be obtained and associated with your PassKey or Passkey for Mobile. If an expired certificate is no longer needed, it can be deleted.

Tip: To see the date a certificate was issued, click the certificate name to open Certificate Details.

Import a certificate

If a certificate is available in a file, you can import the certificate for use with your PassKey or PassKey for Mobile using the **Import** function in Dashboard's Certificates tab. Certificate files typically have a .pfx or .p12 extension.

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:

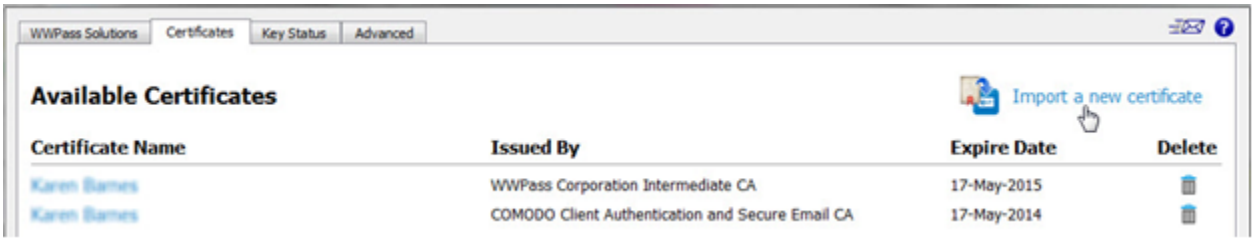
- Remove the certificate file from your computer. At this point, the certificate is securely stored in WWPass cloud storage, where it is encrypted, fragmented, and dispersed.

To import a certificate

1. Connect your PassKey or Passkey for Mobile to your computer. This ensures the certificate is associated with your PassKey/PassKey for Mobile.

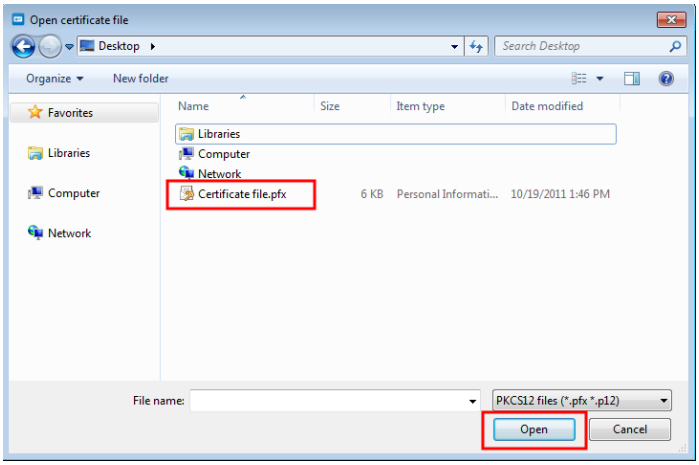
2. Click Dashboard's Certificates tab. Certificate information is retrieved.

3. Click **Import a new certificate**  at the top of the tab.

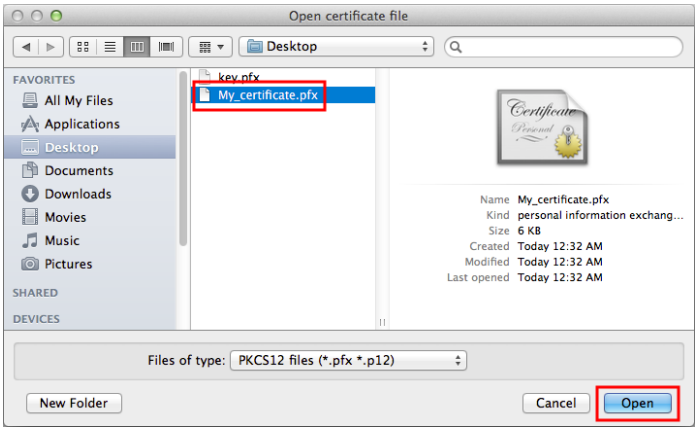


4. From the Open Certificate File window, find the certificate file on your computer. It might have a .pfx or .p12 extension. Select the file and click  :

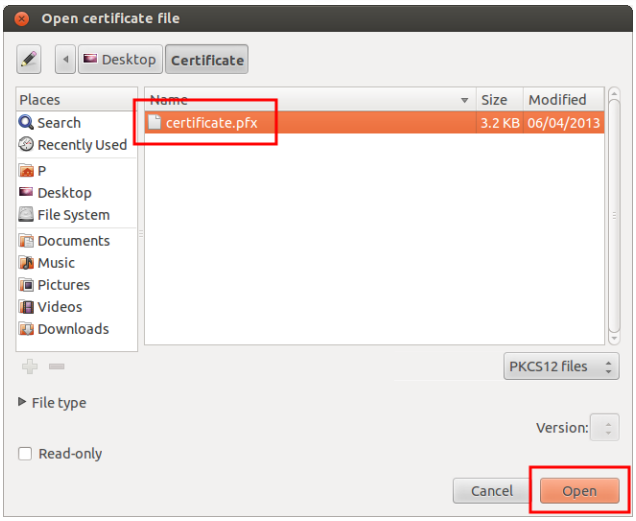
Open Certificate File window on Windows:



Open Certificate File window on Mac:

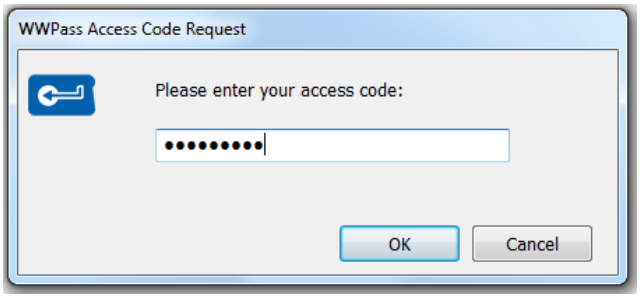


Open Certificate File window on Linux:



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/Passkey for Mobile and click OK. The certificate is imported and shown in Dashboard's Certificate tab.



Delete a Certificate

You can delete a certificate using the **Delete** function in Dashboard's Certificates tab.

This function should **only be used for** certificates that:

- Are no longer needed.
- Have expired.
- Were associated with your PassKey/PassKey for Mobile in error.

Once a certificate is deleted, it cannot be used for authentication with your PassKey/PassKey for Mobile. You will no longer have access to the service, application, or site the certificate was for unless you:

- Obtain a new certificate and associate it with your PassKey/PassKey for Mobile.
- Have another way to authenticate, such as a username and password.

To delete a certificate

1. Connect your PassKey/PassKey for Mobile to your computer.
2. Click Dashboard's Certificates tab. Certificate information is retrieved.
3. Click the **Delete** icon at the end of the certificate's row.
4. When a message asks if you are sure you want to delete certificate, click OK.
5. When prompted, enter the access code for your PassKey/PassKey for Mobile and click OK. The certificate is deleted. The delete process might take some time.

CHAPTER 6 — KEY STATUS TAB

This chapter covers using the Key Status tab in the WWPass Dashboard.

Topics In This Chapter

- Overview
- Using the Key Status Tab
- Status Reference Chart

Overview for the Key Status Tab

The Key Status tab shows the status of the PassKey for Mobile or the Keys in your WWPass KeySet—PassKey and Service Keys. The tab also shows general information and internal technical information for your Key or Keys:

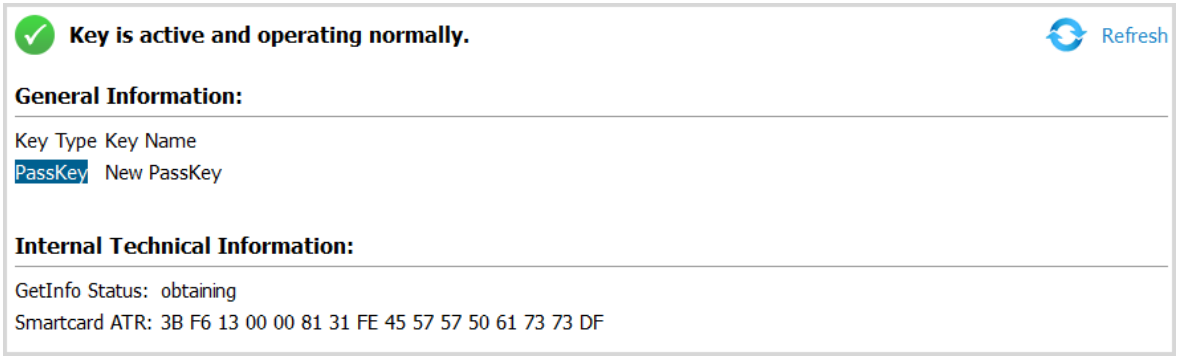
General Information identifies which Key in a KeySet is currently presented to your computer.
It consists of:

- **Key Type**—This is either PassKey (Passkey for Mobile) or Service Key.
- **Key Name**—This is the name you specified when you activated the Key in Key Services.

Internal Technical Information might be needed for advanced troubleshooting if you contact the WWPass Service Desk. The same information is shown for Services Keys. It consists of:

- **GetInfoStatus**—This is a status code returned by the PassKey's Smart Card. PassKeys use Smart Card technology for a number of WWPass solutions.

- **Smart Card ATR**—This is the Smart Card ATR (Answer to Reset) output for a PassKey. ATR conveys information about communication parameters and state for a Smart Card following electrical reset of its chip by a Smart Card reader. The presence of an ATR is one indication that the card is operative. The ATR string identifies who made or issued a PassKey's Smart Card.

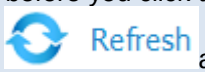


Using the Key Status tab

Follow the steps below to check status and information for one or more Keys in your WWPass KeySet or for your Passkey for Mobile.

To check Key status

1. Connect a PassKey/PassKey for Mobile or Service Key to your computer.
2. Click Dashboard's Key Status tab.

   Note: If a Key is not connected before you click the tab, "No Key present" is shown. Connect a Key to your computer. Then click 

   at the top of the tab.

3. Click 

 in the message that asks to allow authentication into Key Services. Key information is retrieved and displayed in the Status tab.
4. If you want to check status for another Key, disconnect the Key currently presented. Information on that Key is cleared from the tab and "No Key present" is shown.
5. Connect the other Key to your computer. Then click 

 at the top of the Key Status tab.
6. Click 

 in the message that asks to allow authentication into Key Services. Key information is retrieved and displayed in the Status tab.

Status Reference Chart

Status	What It Means	What To Do
Blank PassKey	Shown for a PassKey/Passkey for Mobile that has not been activated.	Activate your KeySet from WWPass Key Services: https://ks.wwpass.com/
Blank Service Key	Shown for a Service Key that has not been activated.	Activate your KeySet from WWPass Key Services: https://ks.wwpass.com/
Key has an internal error	Shown when a problem has occurred with a Key's software or hardware.	Please contact info@wwpass.comfor assistance.
Key is active and operating normally	Shown when there are no problems with a Key.	Use your Key as normal.
Key is blank	Shown when a Key has not been configured as a PassKey/Passkey for Mobile or Service Key.	Activate your KeySet from WWPass Key Services: https://ks.wwpass.com/
Key is not initialized	Shown when a Key has not been configured as a PassKey/PassKey for Mobile or Service Key.	Activate your KeySet from WWPass Key Services: https://ks.wwpass.com/
Key is not initialized properly	Shown when something went wrong during Key activation.	Contact the WWPass Service Desk for assistance. Click here for contact methods.
Key is disabled	Shown when a Key was disabled from Key Services. You can disable a Key if it was lost or stolen.	If the Key is found, you can activate it from WWPass Key Services: https://ks.wwpass.com/
No Key present	A PassKey/PassKey for Mobile or Service Key is not connected to your computer.	Connect your PassKey/PassKey for Mobile or Service Key to your computer by placing it on or near your NFC reader/inserting it into a USB port or pairing it with your computer in case with PassKey for Mobile. Then click Refresh to obtain the Key's status.
Unknown device detected	Shown when a device other than a PassKey/Passkey for Mobile is connected to your computer. Examples of other	Connect your PassKey/Passkey for Mobile or Service Key to your computer by placing it on or near your NFC reader/inserting it into a USB port or pairing it with your computer in case with PassKey for Mobile. Then click

	devices include smart cards for public transportation and mobile phones.	Refresh to obtain the Key's status.

CHAPTER 7 — ADVANCED TAB

This chapter covers using the Advanced tab in the WWPass Dashboard.

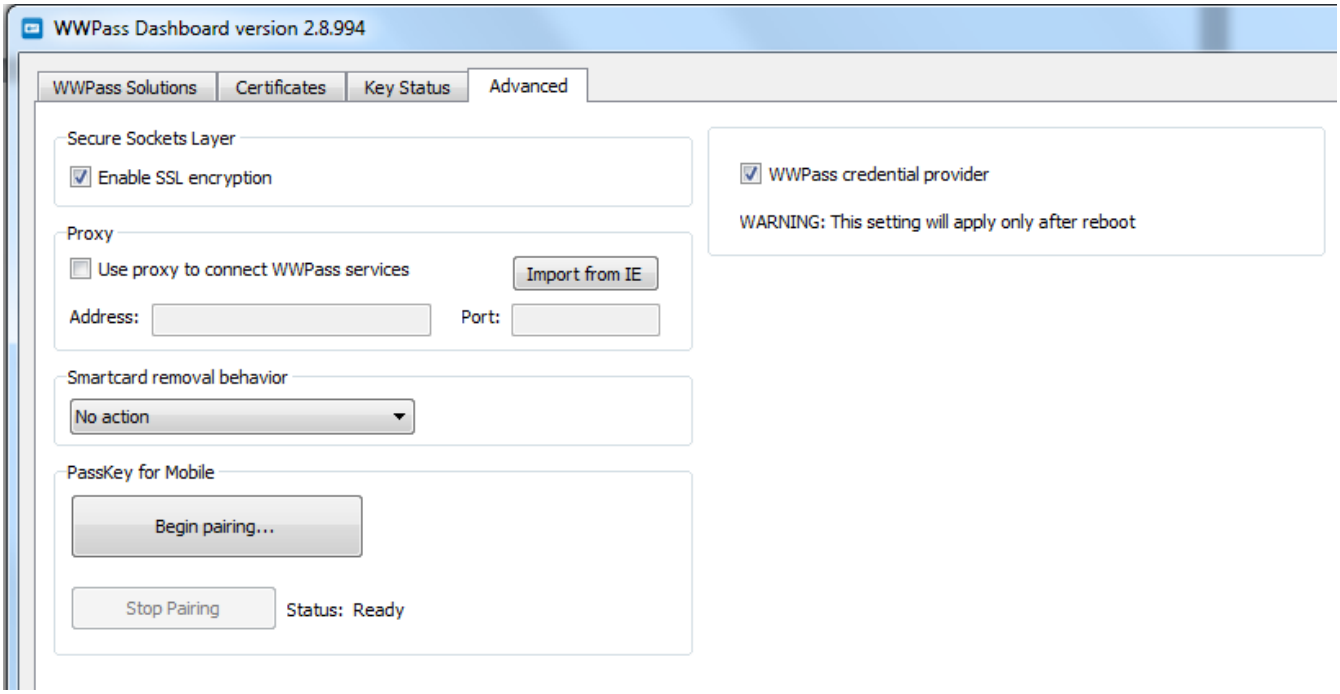
Topics In This Chapter

- Overview
- Use the SSL Encryption Feature
- Use the HTTP Proxy Feature
- Use the Smart Card Removal Feature
- Use the WWPass Credential Provider Feature
- PassKey for Mobile Pairing

Overview for the Advanced Tab

The Advanced tab provides advanced settings that let you:

- Control use of SSL encryption for communication with WWPass services. Click here for information.
- Determine whether an HTTP proxy server is used for communication with WWPass services. Click here for information.
- Determine what happens when a PassKey or PassKey for Mobile is disconnected from a Windows computer while you are logged in. Click here for information.
- Allow Windows logon with a PassKey or Passkey for Mobile from a remote location. Click here for information.
- Allow PassKey for Mobile pairing from WWPass Dashboard. Click here for information.

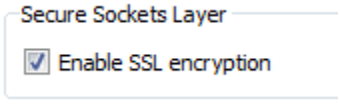


Using the Enable SSL Encryption Feature

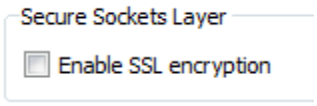
By default, the HTTPS protocol is used for all communication between your PassKey/PassKey for Mobile and WWPass services. You can control whether the HTTPS or HTTP protocol is used for certain parts of this communication using the **Enable SSL encryption** feature.

To use the SSL encryption feature

1. Set the **Enable SSL encryption** checkbox as follows:



Select the checkbox when your system prevents use of the HTTP protocol. The HTTPS protocol and SSL encryption will be used for all communication between your PassKey/PassKey for Mobile and WWPass. (The checkbox is selected by default.)



Clear the checkbox when your system allows use of the HTTP protocol and you want to speed up communication between your PassKey/PassKey for Mobile and WWPass. HTTPS is used only for communication that requires the security of SSL encryption. HTTP is used for all other communication.

What are HTTP and HTTPS?

HTTP (Hypertext Transfer Protocol) is a set of rules for transferring data on the World Wide Web. It is the application protocol in the TCP/IP suite of protocols for the Internet. When a user opens their Web browser, they indirectly make use of HTTP.

HTTPS stands for HyperText Transfer Protocol over SSL (Secure Socket Layer). It is a TCP/IP protocol used by Web servers to transfer and display data securely. Data is encrypted so that it can only be read by the recipient.

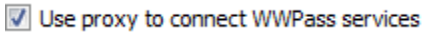
Using the HTTP Proxy Feature

The **Use proxy to connect WWPass services** feature lets you control whether your PassKey/PassKey for Mobile communicates with WWPass Services over the Internet via an HTTP proxy server.

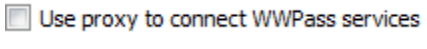
Note: Internet connections are made through a proxy server primarily at organizations and companies. Typically, people connecting to the Internet from home do not use a proxy server.

To use the HTTP proxy feature

1. Set the **Use proxy to connect to WWPass services** checkbox as follows:

   Select the checkbox if you want Internet connections between your PassKey/PassKey for Mobile and WWPass to be made through an HTTP proxy server.

   Clear the checkbox if you do not use a HTTP proxy server for Internet connections. You do not need to perform remaining steps. (The checkbox is not selected by default.)

2. In the **Address** box, enter the address of the proxy server, for example: proxy.example.net

3. In the **Port** box, enter the number of the port used for HTTP connections, for example: 80

   Note: If Internet Explorer is your web browser, you can automatically enter address and port by clicking Import from IE. If a proxy configuration is not available, the "No active proxy configuration found" message appears.

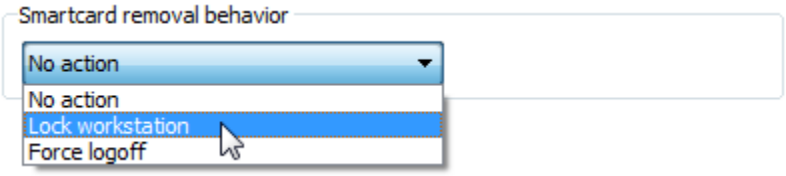
Using the Smart Card Removal Feature

The **Smartcard removal behavior** feature is for use with WWPass Security for Windows Logon.

It lets you control what happens when you disconnect your PassKey/PassKey for Mobile after using it to log into a Windows Active Directory domain. You can choose to lock your computer, automatically log out of Windows, or remain logged into Windows when your PassKey/PassKey for Mobile is disconnected.

Locking your computer and logging out are the most secure behaviors in a work setting when you plan to leave your computer unattended.

You need administrative rights for your computer in order to change Smart Card removal behavior.



Note: At an organization or company, the default behavior for SmartCard removal can be set by a system administrator using the **Interactive logon: Smart card removal policy** group policy. The setting you select in Dashboard might override the default behavior.

To use the Smartcard removal feature

1. Click in the list below **Smartcard removal behavior** and select a setting as follows:
   - **No Action**—Select this if nothing should happen when you disconnect your PassKey or PassKey for Mobile from your Windows computer. You remained logged into Windows.
   - **Lock workstation**—Select this to automatically lock your computer when you disconnect your PassKey or PassKey for Mobile from your Windows computer. This ensures that your computer cannot be accessed while you are away from it. Your current Windows session is not ended. You can resume the session using the Ctrl + Alt + Delete keys.
   - **Force logoff**—Select this to automatically log out of Windows when you disconnect your PassKey or PassKey for Mobile. Your current Windows session is ended. To log on again, you need to connect your PassKey or PassKey for Mobile to your computer and enter its access code.

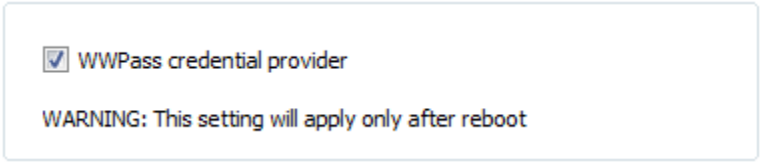
     Note: If you are logged in as a user without administrative rights for the computer, you are prompted to log in as an administrator. If you cannot log in as an administrator, you cannot change Smartcard removal behavior. Ask a system administrator to do this for you.

Using the WWPass Credential Provider Feature

The **WWPass credential provider** feature is for use with WWPass Security for Windows Logon.

It lets you choose which Credential Provider to use for PassKey/PassKey for Mobile logon to Windows. You might use the WWPass Credential Provider under most circumstances. You can use the Windows SmartCard Credential Provider for logon from a remote location that does not have access to the corporate network and Microsoft Active Directory.

You need administrator rights for your computer in order to change the Credential Provider.



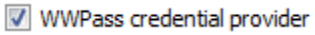
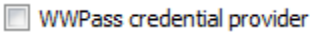
Here's more information about the two Credential Providers available:

- **WWPass Credential Provider**—This is selected by default and supports PassKey/PassKey for Mobile logon when you can connect to the corporate network and Active Directory. When you press Ctrl + Alt + Delete to log into Windows, the WWPass Logon tile appears.

- **Windows Smart Card Credential Provider**—You can switch to this Credential Provider when you want to use a PassKey/PassKey for Mobile for Windows logon from a remote location where you cannot connect to the corporate network. To make the switch, clear the **WWPass credential provider** checkbox. This should be done while you are still connected to the corporate network, before you log in from the remote location. When you press Ctrl + Alt + Delete to log into Windows, the Insert a Smart Card tile appears.

To use the WWPass credential provider feature

1. Set the **WWPass credential provider** checkbox as follows:

	Select the checkbox if you want to use the WWPass Credential Provider. (The checkbox is selected by default.)
	Clear the checkbox if you want to use the Windows Smart Card Credential Provider for remote login.

Note: If you are logged in as a user without administrative rights for the computer, you are prompted to log in as an administrator. If you cannot log in as an administrator, you cannot change the Credential Provider. Ask a system administrator to do this for you.

2. Restart your computer to put the setting into effect.

Using the Mobile Key Pairing

To use the PassKey for Mobile feature

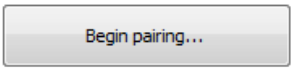
The PassKey for Mobile feature is available only on Windows and lets you pair your smartphone with a computer to connect it to your PC and start using it as a PassKey.

After the application setup has successfully been finished (click here for the steps to follow to install the application on your smartphone), you will see the WWPass application icon on your smartphone screen.

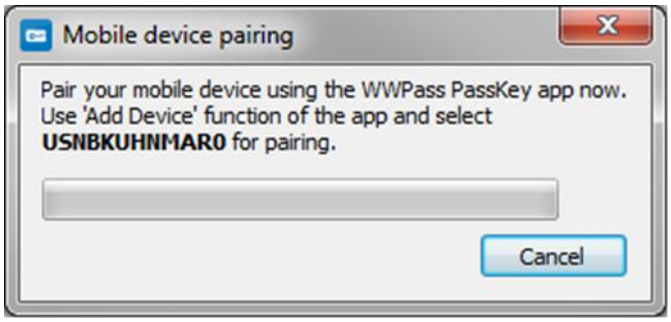
After you tap the WWPass PassKey for Mobile application icon on the smartphone screen, you will see the notification that your device has not been paired with your computer.

Note: Make sure you have turned on Bluetooth or WiFi on your computer and that your smartphone and computer are connected to the same WiFi network.

To pair your smartphone with a computer:

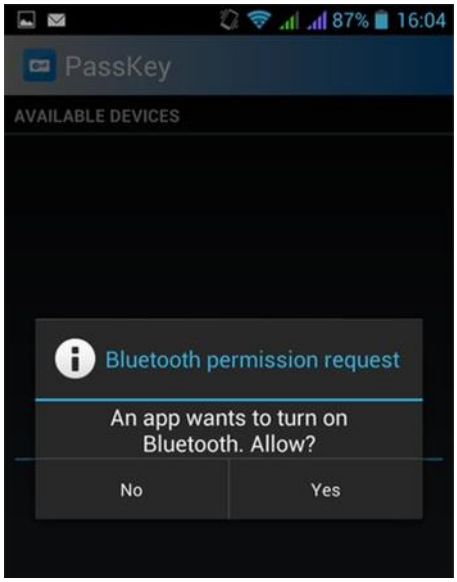
1. Download and install the Security Pack from Key Services at https://ks.wwpass.com/download/ .
2. Open the WWPass Dashboard, click the Advanced tab and press 

. The Smart Device Pairing dialog will appear.



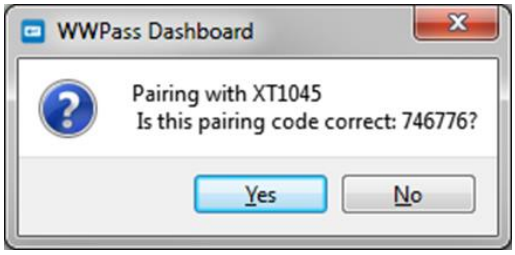
3. Tap either the  icon at the top of your smartphone screen or the 

button.
4. You will see the Bluetooth permission request on your smartphone, if it has not been turned on, click “Yes” to allow.

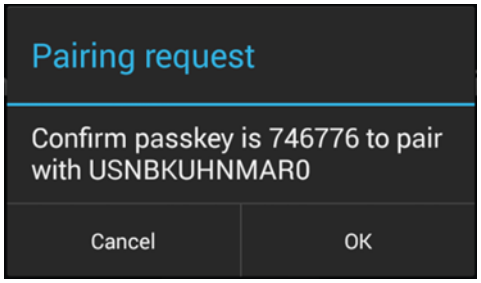


5. You will see the name of your computer in the available device area. Tap the available device. You see the pairing request on your smartphone.

6. Compare the pairing code of your smartphone with the code indicated in Dashboard on the computer. Click “Yes”, if the smartphone code is consistent with the computer code.



7. Tap “OK” to confirm the request if the name of your computer is consistent with the name shown on your smartphone screen.



8. In the Known Devices list, you will see the computer name and either a WiFi  icon or a standard Bluetooth  icon depending on how your smartphone is connected. The WiFi icon will appear green when connected. The Bluetooth icon will appear blue when connected. The Dashboard icon will appear blue  indicating that your mobile PassKey is successfully connected.

Note: You need to pair your smartphone to a computer or a laptop only one time. When you want to use your smartphone as a PassKey, connect it to your computer by tapping the computer name and “Yes” in the confirmation window.

PassKey for Mobile activation

Note: If you have paired your smartphone with your computer, be sure it is disconnected before you start activation.

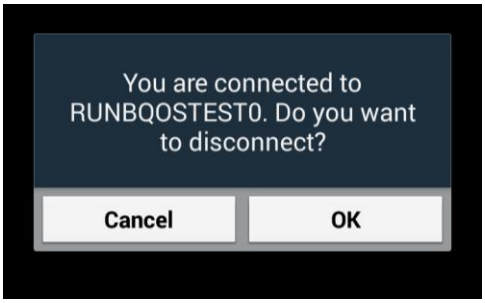
Now that your smartphone has been paired you can activate and start using it as a PassKey.

Click here for the steps to follow:

- If you have a PassKey for Mobile only, with no Service Keys (Personal and Standard Editions)
- If you want to use your PassKey for Mobile with your current KeySet with two service Keys (Pro Edition)
- If you want to activate your KeySet with a PassKey for Mobile instead of a hardware PassKey

Note: If you just paired your smartphone with the computer, make sure you disconnected it before either creating an extra PassKey or activating a new KeySet and be sure to insert your Service Key first.

To disconnect your smartphone, tap the device it was connected to and click “OK” to confirm the disconnection in the dialog window.



CHAPTER 8 — UPDATE THE SECURITY PACK

This chapter covers how to update WWPass Security Pack from the WWPass Dashboard.

Topics In This Chapter

- Overview
- Update the WWPass Security Pack

Overview for Updating the WWPass Security Pack

Updating the WWPass Security Pack updates all of its components, including the WWPass Dashboard.

On Windows and Mac, the Security Pack can be updated from Dashboard or from WWPass Key Services: https://ks.wwpass.com/download/

On Linux, the Security Pack can be updated from the WWPass Linux Repository. Instructions are available in Key Services.

In order to update the Security Pack on any platform, you must have administrator rights for your computer.

Because updates via Dashboard are done over the Internet, Dashboard can only be used when Internet access is not restricted by security policies, a firewall, or the IT department. If Internet access is restricted, you need to use Key Services for updates.

Using Dashboard for updates is covered in this user guide. Using Key Services is covered in KeySet help.

Note: Dashboard is initially installed as part of the WWPass Security Pack.

Steps to follow

Click links below for information on how to update the Security Pack:

- Click here for steps to follow on Windows
- Click here for steps to follow on a Mac
- Click here for steps to follow on Linux

How to tell if an update is needed

By the Dashboard key icon in the system tray on Mac and Windows you can tell, whether the Security Pack needs an update:

- When the current version is installed, a key icon is blue and a key icon is grey when your PassKey/PassKey for Mobile is not connected to your computer.
- When an update is needed, a key icon with an exclamation point is shown in the system tray.

On Linux platform Security Pack is updated automatically. Click here for steps to follow if you want to update Linux manually.

Update the WWPass Security Pack on Windows

Follow the steps below to update the WWPass Security Pack on Windows from the WWPass Dashboard. You must have administrator rights for your computer.

To update the Security Pack on Windows

1. Click the icon key with a red exclamation point in the system tray. Click Install Now to confirm installation of a new Security Pack version, click Update Later to postpone installation.

2. Click OK in the message that tells you Dashboard will close in order to install the update. The setup wizard opens.

3. From the Welcome screen, click Next to begin updating the Security Pack.

4. When the update is complete, the Completed screen appears. In addition, a Dashboard message alerts you that your computer should be restarted. The message appears from the WWPass Key icon in the system tray. Click Finish to close the setup wizard.

5. Restart the computer to enable all Security Pack features. You can then start Dashboard.

Update the Security Pack on a Mac

Follow the steps below to update the WWPass Security Pack on a Mac from the WWPass Dashboard. You must have administrator rights for your computer.

To update the WWPass Security Pack on a Mac

1. Click the  icon key with a red exclamation point in the system tray. Click **Install Now** to confirm installation of a new Security Pack version, click **Update Later** to postpone installation.

2. Click 

in the message that tells you Dashboard will close in order to install the update. The WWPass Security Pack Installer opens.

3. From the “Welcome” screen, click **Continue** to begin updating the WWPass Security Pack.

4. From the “Important Information” screen, note text about restarting your computer after the update is complete. Then click **Continue**.

5. From the “Standard Install” screen, click **Install** to begin updating the Security Pack. Then click **Continue Installation** in the message that asks if you’re sure you want to install the software now. Finally, enter your password and click **Install Software**.

6. From the "installation was completed successfully" screen, click **Restart** to restart your computer and enable all features of the Security Pack. You can then start Dashboard.

Update the Security Pack on Linux

Follow the steps below to update the WWPass Security Pack on Linux (Ubuntu 12.04 Precise Pangolin and Ubuntu 14.04 Trusty Tahr) manually.

These steps can be followed if the Security Pack is available in: /etc/apt/sources.list

To update the Security Pack on Linux

1. Close the WWPass Dashboard, if it is currently open.

2. Run:

   ```
   sudo apt-get update
   ```

3. Install the Security Pack using this command:

   ```
   sudo apt-get install wwpass-security-pack
   ```

4. Start Dashboard.