USER GUIDE

WWPass Security for Windows Logon

December 2015

TABLE OF CONTENTS

CHAPTER 1 — WELCOME

This chapter introduces WWPass Security for Windows Logon 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 Windows Logon

This documentation covers how to set up and use WWPass Security for Windows Logon, the WWPass authentication solution for Microsoft Windows.

WWPass Security for Windows Logon allows you to log into a corporate Windows domain using a PassKey instead of a username and password. You can then access all files and applications you have permissions for on the Windows network.

PassKey authentication is certificate based and uses Smart Card technology. During setup, an X.509 certificate for your Windows domain is associated with your PassKey. The certificate is stored in WWPass secure cloud storage, where it cannot be stolen.

Click here for more information.

Note: WWPass Security for Windows Logon is part of the WWPass Security Pack and is shown in the WWPass Dashboard on Windows computers. The Security Pack allows you to activate a PassKey and use WWPass authentication solutions. Dashboard shows you the solutions included in the Security Pack.

Related Documentation

This documentation provides information on WWPass Security for Windows Logon for system administrators and 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	PDF
WWPass Security Pack	PDF
Installation	
Windows	PDF
Mac	PDF

Linux	PDF
WWPass Dashboard for Security Pack	PDF
WWPass Solutions for Security Pack	
WWPass Security for Email (Outlook & OWA)	PDF
WWPass Security for Email (Thunderbird)	PDF
WWPass Security for Firefox	PDF
WWPass Security for VPN (Juniper VPN)	PDF
WWPass Security for VPN (OpenVPN)	PDF
WWPass Security for Windows Logon	Currently open
WWPass Security for SharePoint	PDF
Personal Secure Storage	
Windows	PDF
Mac	PDF
Linux	PDF

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 PassKey to your 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 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 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 WWPass Product Support Desk as follows:

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

Report a Problem from Dashboard

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

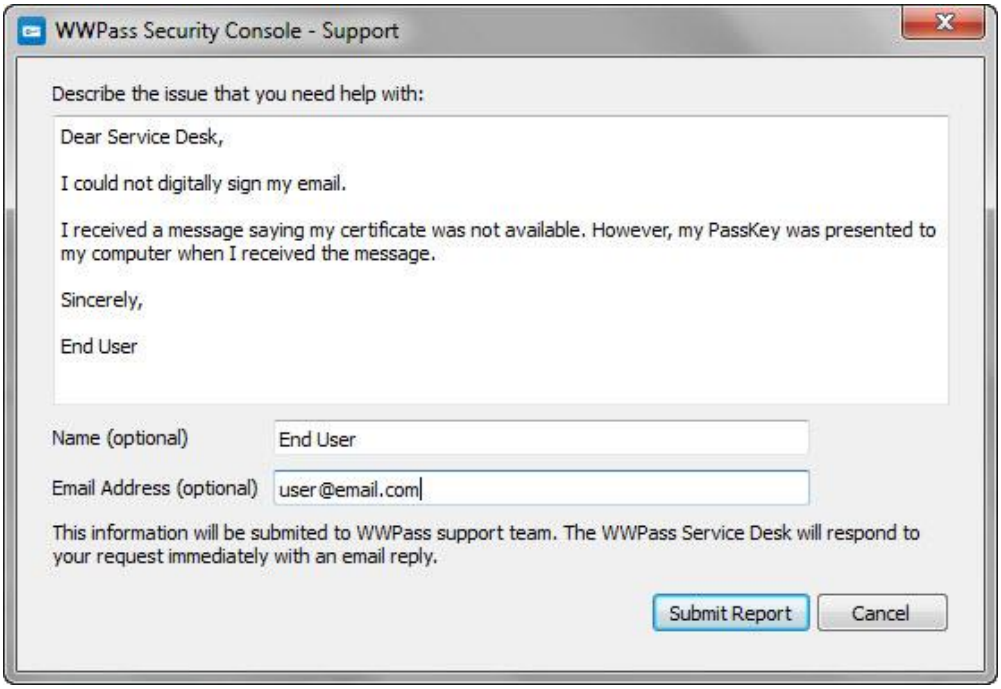
The email identifies version numbers for Security Pack and operating system. In addition, the current logs for WWPass software are automatically attached to the email.

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.

Logs are located in Users\username and ProgramData. They 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 Submit Report to send your report along with the current version of all available logs.



CHAPTER 2 — REQUIREMENTS

System Requirements

Requirement	Details
Windows Server and domain-based network	Windows Server 2008 and 2008 R2, 2012 and 2012 R2 (32-bit and 64-bit) are supported. **Note:** Support for Smartcard Mini Driver Specification version 6 or higher is required.
Smart Card logon enabled	Smart Card logon is used by the PassKey and should be enabled for the domain controller server.
Internet access	Outbound TCP connections must be allowed from user computers to ports 80 (HTTP) and 443 (HTTPS). Network software and hardware (including routers and firewalls) should not block outbound connections to these ports.
Certificate Authority (CA)	A CA is needed to issue digital X.509 certificates for user authentication into your Windows domain. This documentation describes using the Microsoft Enterprise CA to issue domain-based, self-signed certificates that are trusted within your organization. Users enroll for certificates via the web using Active Directory Certificate Services (included with Windows Server).

User Requirements

Requirement	Details
Computer with Windows operating system	The following versions of Microsoft Windows are supported: • Windows 10 (32-bit and 64-bit) • Windows 8.1 (32-bit and 64-bit) • Windows 8 (32-bit and 64-bit) • Windows 7 (32-bit and 64-bit) **Note:** Support for Smartcard Mini Driver Specification version 6 or higher is required. **Note:** Outbound TCP connections must be allowed to ports 80 (HTTP) and 443 (HTTPS).
Windows account	You need a Windows domain account in Microsoft Active Directory to log into your Windows network.
Web browser	The following browsers are supported: • Microsoft Internet Explorer 8 and later (32-bit and 64-bit) • Chrome 20 and later • Firefox 14 and later • Opera 11 and later
Certificate for Windows domain	This a digital X.509 certificate from the Certificate Authority (CA) used by your organization. It serves as a credential that authenticates your identity when you log onto your Windows domain with a PassKey.
WWPass KeySet	This includes the PassKey used for authenticating into Windows. Click here for information on obtaining a KeySet.
WWPass Security Pack	This includes WWPass Security for Windows Logon and software that is needed to activate your KeySet. Click here to open Security Pack help.

CHAPTER 3 — SETUP FOR ADMINISTRATORS

This chapter covers setup for system administrators. It includes information on essential tasks that must be performed before users can log onto Windows using a PassKey.

For complete information on Windows authentication, see Microsoft documentation.

Topics in This Chapter

Smart Start for Administrators

This Smart Start is an overview of the main setup steps for system administrators. It provides a road map to follow as you go through the setup process.

Smart Start

1. Prepare for issuing certificates to Windows users. Certificates authenticate users when they log onto Windows with their PassKeys.

2. Set local Smart Card policies for users across the domain (PassKeys use Smart Card logon):

3. Set Smart Card Group Policies for user computers across the domain (PassKeys use Smart Card logon):

   - Set startup type for the Smart Card service and Smart Card Removal Policy service. Also make sure the Smart Card service is started.

   - Set behavior for the Windows' Smart Card Removal Policy security setting. This determines what happens when users remove their PassKey from their computer. The behavior can be to lock the workstation, force logoff, disconnect for a remote desktop services session, or no action.

4. Set up a PassKey for your own use:

   a) Install WWPass Security Pack on your computer. Click here for Security Pack help.

   b) Obtain and activate a WWPass KeySet. This includes a PassKey. Click here for KeySet help. (If you are currently using another WWPass solution, your KeySet is already activated.)

   c) Obtain a certificate for your Windows domain and associate it with your PassKey. Present your PassKey to your computer before you begin.

Tip: Click here for the setup needed if you want to use your PassKey to log into Windows from a remote location.

Prepare to Issue Certificates from a CA

This topic provides guidelines on setting up to issue digital X.509 certificates from an internal Certificate Authority (CA).

The guidelines are for a Microsoft CA server on your Windows domain. Certificates issued by the CA are self-signed by your organization and trusted within your organization.

Users request certificates via their browsers from Active Directory Certificate Services (included with the server.)

An Active Directory Domain Controller is used for user authentication.

For more information, see Microsoft documentation.

Note: You can also use an external third-party CA such as Comodo. For more information, see Microsoft documentation on third-party certificates.

Guidelines

1. Select the Active Directory Certificate Services role from Server Manager for Windows Server. Also select the following role services:
   - Certification Authority (issues certificates).
   - Certification Authority Web Enrollment (provides the Active Directory web interface for certificate enrollment).

2. Configure the Smart Card template for the CA. The template's default setting for CSP (Cryptographic Service Provider) should be **Microsoft Base Smart Card Crypto Provider**. (This setting associates a certificate with a user's PassKey.) Users select Smart Card as the Certificate Template in Certificate Services when they request a certificate.

3. For the Active Directory Domain Controller that will authenticate users, make sure:
   - Smart Card authentication is enabled.
   - A Domain Controller certificate is installed. This should be valid for your Active Directory domain.
   - The Domain Controller trusts the Certificate Authority (CA) used to issue X.509 certificates to users. (User computers must trust the root CA.)
   - The HTTPS protocol is bound to the IIS server.

Set Smart Card Group Policies

This topic covers how Smart Card Group Policies should be set for PassKey authentication into Windows. The required settings are as follows:

- **Smart Card Service**—Startup type for this should be Automatic. In addition, the service should be started. If this service is stopped on a user computer, the computer will not be able to read the user's PassKey. The Smart Card service is shown as SCardSvr in Windows Task Manager.

- **Smart Card Removal Policy Service**—Startup type for this should be automatic. This allows you to set Smart Card removal behavior (see next setting). The Smart Card Removal Policy service is shown as SCPolicySvc in Windows Task Manager.

- **Interactive logon: Smart card removal policy**—This setting determines what happens when users remove their PassKey from their computer while they are logged into Windows. Options are as follows:

  - **No Action**—Select this if nothing should happen and users should remain logged in when they remove their PassKey. This is the least secure behavior as user computers are not locked and Windows sessions are not disconnected.

  - **Lock Workstation**—Select this if computers should be locked automatically when users remove their PassKey. This ensures that a computer cannot be accessed while a user is away from it. The current Windows session is not ended.

  - **Force Logoff**—Select this if computers should be logged out of Windows automatically when users remove their PassKey. The current Windows session is ended. To log on again, users must present their PassKey again and enter its access code.

  - **Disconnect if a Remote Desktop Services session**—Select this to automatically disconnect remote Windows sessions when users remove their PassKey. Users are not logged off. (If a session is local, the computer is locked.) To resume a session, a user can present their PassKey to the same computer or another computer with a Smart Card reader. They do not need to log on again.

Note: Another security setting for Smart Cards is **Interactive Logon: require Smart Card**. When the setting is disabled (the default and recommended setting), users can log on using any method supported by your company, including Smart Card logon with a PassKey. When the setting is enabled, users can only use Smart Card logon with a PassKey.

CHAPTER 4 — SETUP FOR USERS

This chapter covers setup for users. It includes information on essential tasks that must be performed before you can log onto Windows using a PassKey.

Topics in This Chapter

Smart Start for Users

This Smart Start is an overview of the main setup steps for users. It provides a road map to follow as you go through the setup process.

Smart Start

1. Install WWPass Security Pack on your computer. Click here for Security Pack help.

2. Obtain and activate a WWPass KeySet. This includes a PassKey. Click here for KeySet help. (If you are currently using another WWPass solution, your KeySet is already activated.)

3. Obtain a certificate for Windows and associate it with your PassKey. Present your PassKey to your computer before you begin.

   Tip: Click here for the setup needed if you want to use your PassKey to log into Windows from a remote location.

Obtain a Certificate

Ask a system administrator how to obtain a certificate and associate it with your PassKey. The certificate serves as a credential that proves your identity when you log onto Windows.

The steps below provide an example of how to obtain a certificate via Microsoft Active Directory Certificate Services. Steps at your company might be different.

Before you begin, ask a system administrator for:

- The URL for your company's Certificate Authority (CA).
- Any special settings to select when you request a certificate.

If your certificate is available in a file, you can import it to your PassKey using the WWPass Dashboard, which is included in the WWPass Security Pack.

Note: If the Certificate Authority's root certificate for your domain is not trusted by your computer, Active Directory Certificate Services displays a message that says your root CA is not trusted. Click the link provided to install the root CA on your computer.

To obtain a certificate via Active Directory

1. Present your PassKey to your computer. This ensures your certificate is associated with your Passkey.

2. Open the Internet Explorer web browser from your computer and go to Active Directory Certificate Services using the URL provided by an administrator, for example:

   https://pki.companyname.net/certsrv

3. From the CA Welcome page, click **Request a certificate**.

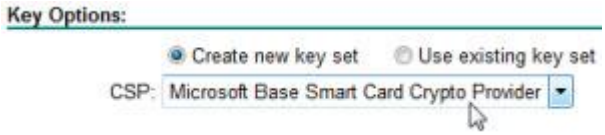
4. From the Advanced Certificate Request page, click **Create and submit a request to this CA**.

Options are displayed.

5. Select options and submit your certificate request as follows:

   a) Select the **Smartcard Logon** template from the **Certificate Template** list.

   b) Select **Microsoft Base Smart Card Crypto Provider** from the **CSP** list. This setting associates the certificate with your PassKey.

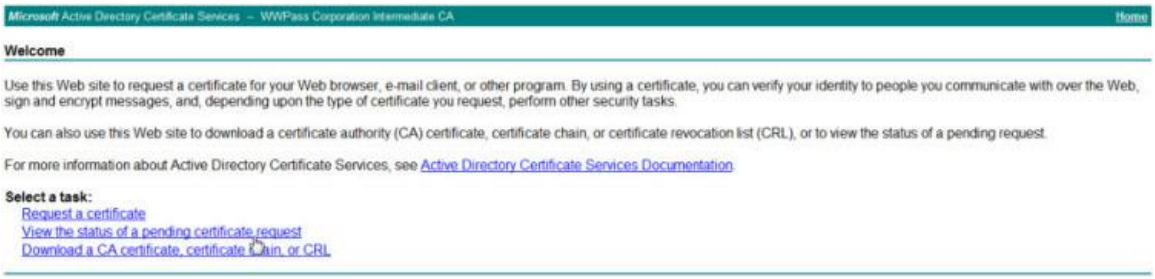


   c) Select **Create new key set** and clear the checkbox for **Mark keys as exportable**. Select other settings based on instructions from an administrator.

   d) Click Submit > to request a certificate. After your request is "generated", enter the access code for your PassKey in the prompt that appears:

   - If certificate requests are automatically approved, your certificate is associated with your PassKey right away. You can now use your PassKey to log onto Windows.
   - If certificate requests are explicitly approved, the Certificate Pending page appears with your Request ID and instructions. Go to the next step.

6. Return to Active Directory Certificate Services to check the status of your request. Click **View the status of a pending certificate request**.



Next click the date link for the certificate.

7. When "Certificate Issued" is shown as the status, click **Install this certificate**. Then enter the access code for your PassKey in the prompt that appears. Your certificate is associated with your PassKey. You can now use your PassKey to log onto Windows.

Import a Certificate

If your certificate is available in a file, you can import the certificate for use with your PassKey. Certificate files typically have a .pfx or .p12 extension.

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

Before you import a certificate:

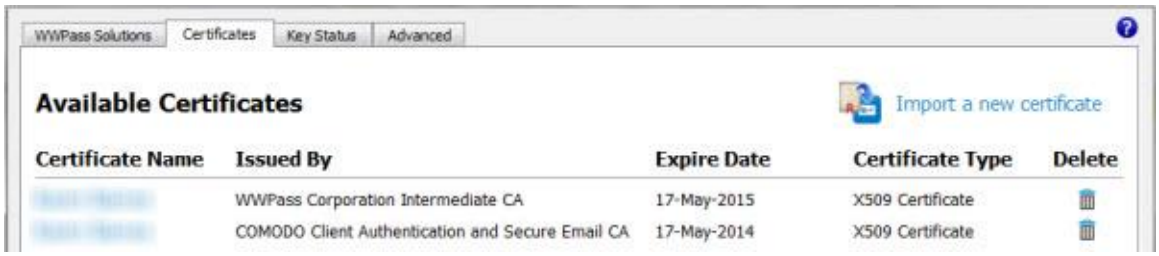
- Put the certificate file in a temporary location on your computer.
- If the file is encrypted, make sure you know the password that was used to encrypt the file.

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.

To import a certificate using the WWPass Dashboard

1. Present your PassKey to your computer. This ensures that the certificate is associated with your PassKey.
2. Open the WWPass Dashboard using the Key icon in the system tray.
3. In the Certificates tab, click the **Import a new certificate** button.



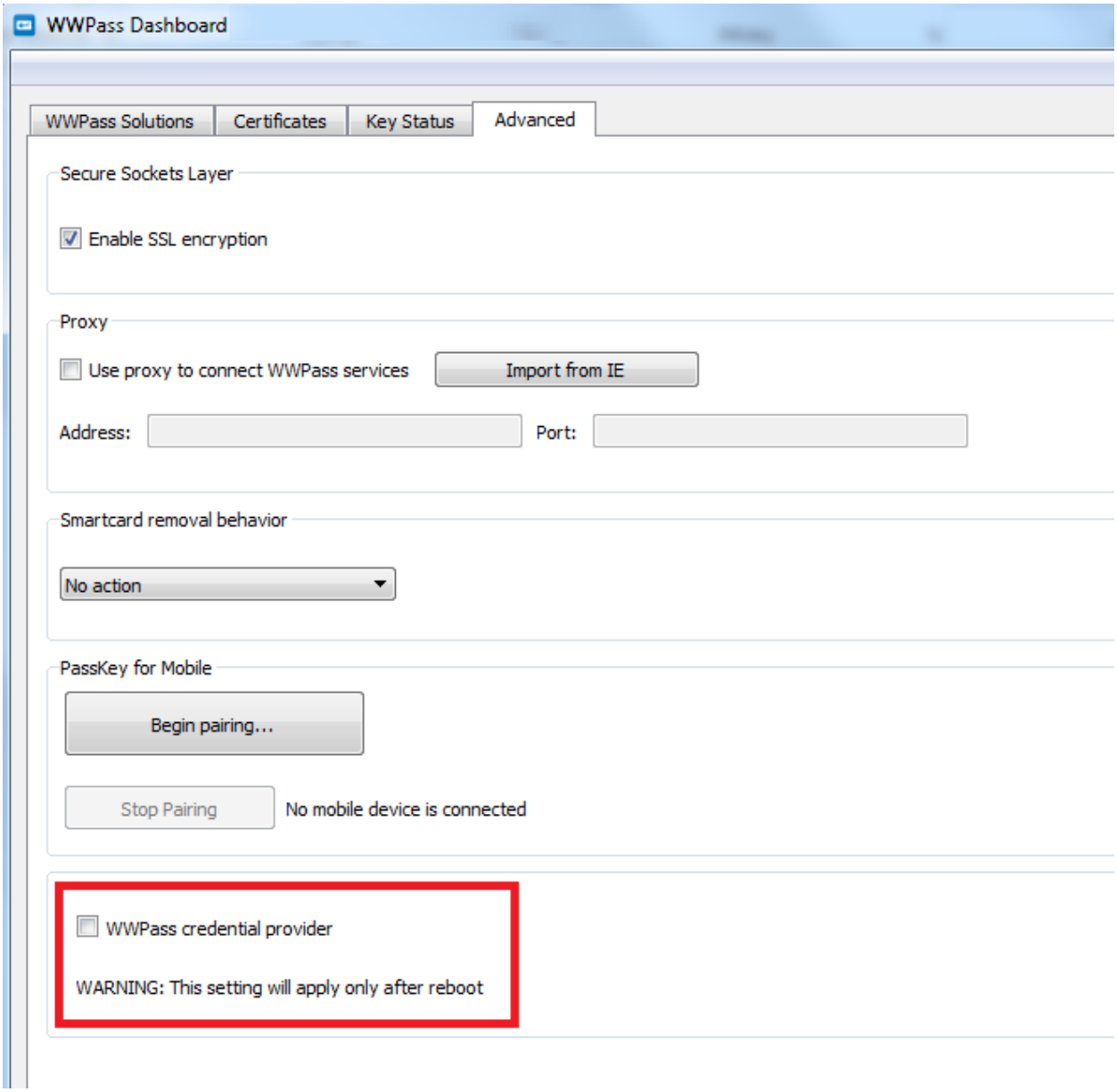
4. From the Open Certificate window, locate the certificate file. Look for an extension of .pfx or .p12. Select the file and click Open.
5. If prompted for the password used to encrypt the certificate file, enter the password and click OK.
6. Enter the access code for your PassKey and click OK.

Set up to Log In from a Remote Location

A little setup is needed if you want to use your PassKey to log into Windows from a remote location that does not have access to the corporate network.

Setup consists of switching to the Windows Smart Card credential provider by clearing the **WWPass credential provider** checkbox in the Advanced tab of the WWPass Dashboard. You need administrator rights for your computer to change the setting for this checkbox.

Setup should be performed while you are still connected to the corporate network, before you log in from a remote location.



Normally, the WWPass credential provide r is used. This supports PassKey logon when you can connect to the corporate network. When you press Ctrl + Alt + Delete to log into Windows, the WWPass Logon tile appears.

If you switch to the Windows Smart Card credential provider, the Insert a Smart Card tile appears when you press Ctrl + Alt + Delete to log into Windows.

To change credential provider

1. Start the WWPass Dashboard from the Windows Start menu.
2. Click the Advanced tab
3. Set the **WWPass credential provider** checkbox as follows:

☑ WWPass credential provider	Select the checkbox if you want to use the WWPass Credential Provider. (The checkbox is selected by default.)
☐ WWPass credential provider	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.

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

CHAPTER 5 — USING PASSKEYS WITH WINDOWS

This chapter covers using a PassKey for Windows logon.

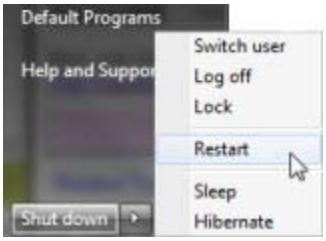
Topics In This Chapter

Overview for Using PassKeys for Windows Logon

Once WWPass Security for Windows Logon is set up, you can use your PassKey to securely log in to Windows and access all content you have permissions for on your Windows network.

Normally, you remain logged on until you shut down your computer. However, you need to log on again and enter your PassKey Access Code if you restart or lock your computer or log off.

The **Restart**, **Lock** and **Log Off** functions are available on the menu that appears when you click the Windows Start button and the arrow next to **Shut down**. After you use any of these functions, you are prompted to press the Ctrl + Alt + Del keys in order to log on.



You might also need to log on again if you remove your PassKey while you are logged onto Windows. This depends on Windows settings selected by a system administrator. See Removing Your PassKey While You Are Logged On.

Log in to Windows Using a PassKey

Follow the steps below to log onto Windows using your PassKey instead of a username and password.

To log onto Windows using a PassKey

1. Start or restart your computer. The Windows logon screen displays the WWPass Logon tile with the **Insert your PassKey** message.

Tip: You can bypass the **Insert your PassKey** message by presenting your PassKey before you start your computer.

2. Present your PassKey to your computer. The Windows logon screen displays the WWPass Logon tile with your username along with tiles for any other logon credentials found (such as the username and password for your Windows domain).

3. Click the WWPass Logon tile. The **Access Code** box is displayed below your username.

4. Enter the Access code for your PassKey in the box provided and click the right arrow beside it. You are logged onto Windows and the network.

What do these messages mean?

The message shown with the WWPass Logon tile can vary based on the following:

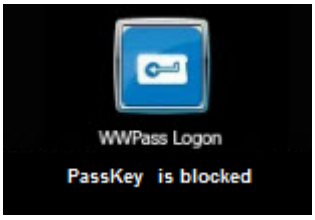
- **Insert your PassKey:** This message is shown when your PassKey is not present when you start or restart your computer. The message is cleared after you present your PassKey. You can bypass the message by presenting your PassKey before you start your computer.

- **Access Code:** The Access Code box is shown when your PassKey is present and valid logon credentials are found. You are logged onto Windows when you enter the access code for your PassKey.

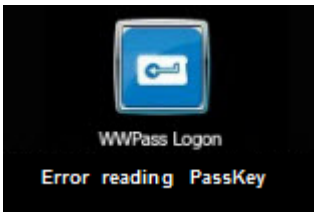
- **Credentials not found/recognized for this domain:** This message is shown when your PassKey is present and logon credentials are found but are not valid for your Windows domain. Contact a system administrator about enrolling for credentials (a certificate) for your Windows domain.

- **No logon credentials found:** This message is shown when your PassKey is present but no logon credentials are found. Contact a system administrator to obtain credentials (a certificate) for your Windows domain. This message can also be shown when your PassKey is currently blocked due to too many logon attempts (three in a row) with the wrong access code. If you were able to log on with your PassKey prior to this, wait 15 minutes for the PassKey to be unblocked.

- **PassKey is blocked:** This message is shown when a PassKey is currently blocked from use. PassKeys are blocked after three authentication attempts with the wrong access code. Use is blocked for 15 minutes. After 15 minutes passes, you can use the PassKey to log on.

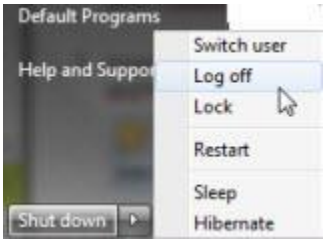


- **Error reading PassKey:** This message is shown when a Service Key or disabled PassKey is presented to the computer for authentication. Present an activated PassKey in order log on.



Log Off Windows

You can log off of Windows by clicking the Windows Start button  , clicking the arrow next to **Shut down**, and selecting **Log off**.



You might be logged off automatically when you remove your PassKey from your computer. This depends on Windows settings selected by a system administrator. See Removing Your PassKey While Logged On.

Removing Your PassKey While Logged On

If you remove your PassKey from your computer while you are logged onto Windows, one of several things can happen:

- **Your computer is locked:** If this happens, your computer is locked so that no one can access it, but you are not logged off of Windows. You can safely leave your desk (take your PassKey with you). To unlock your computer and continue working in Windows, present your PassKey to your computer and enter your PassKey Access Code.
- **You are logged off:** If this happens, you are logged off of Windows. You can safely leave your desk (take your PassKey with you). To log on again, present your PassKey to your computer and enter your Access Code. See Log onto Windows Using a PassKey.
- **You are disconnected from a Remote Desktop Services session:** If this happens, you are disconnected from the remote session but you are not logged off of Windows. To resume the session, present your PassKey to the same computer (or another computer with a Smart Card reader) and enter your PassKey Access Code.
- **Nothing happens:** If nothing happens, you should not leave your computer as anyone can access it and the network content you have permissions for.

What happens when you remove your PassKey depends on how a system administrator has set removal behavior for the **Interactive logon: Smart card removal policy** security setting. You can check this from Administrative Tools in the Windows Control Panel under Local Security Policy > Local Policies > Security Options. However, the setting should not be changed.

Note: If you cannot log on again using your PassKey, use your Windows domain user name and password to log on.