USER GUIDE

WWPass Security for SharePoint

TABLE OF CONTENTS

CHAPTER 1 — WELCOME

This chapter introduces WWPass Security for SharePoint and provides basic information for using a WWPass PassKey to logon to SharePoint.

Topics in This Chapter

Introducing WWPass Security for SharePoint

WWPass Security for SharePoint allows users to log into SharePoint from their web browser (Microsoft Explorer) using a PassKey instead of a username and password. They can then access all content they have permissions for in SharePoint.

This user guide covers how to set up and use WWPass Security for SharePoint. PassKey authentication can be easily integrated into SharePoint implementations that use Smart Card logon and certificates.

Who This Documentation Is For

This documentation contains information for system administrators and end users.

System administrators might want to review all information—information for end users as well as information for administrators.

End users only need to review information for users.

Connecting Your PassKey to Your Computer

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

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

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

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

Need Assistance?

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

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

Report a Problem from the Dashboard

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

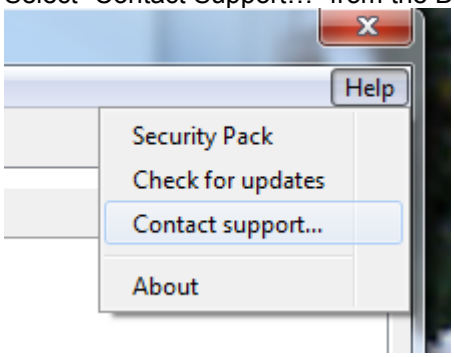
The email identifies version numbers for your Security Pack and operating system. In addition, the current logs for WWPass software are automatically attached to the email.

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

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

To report a problem from the Dashboard

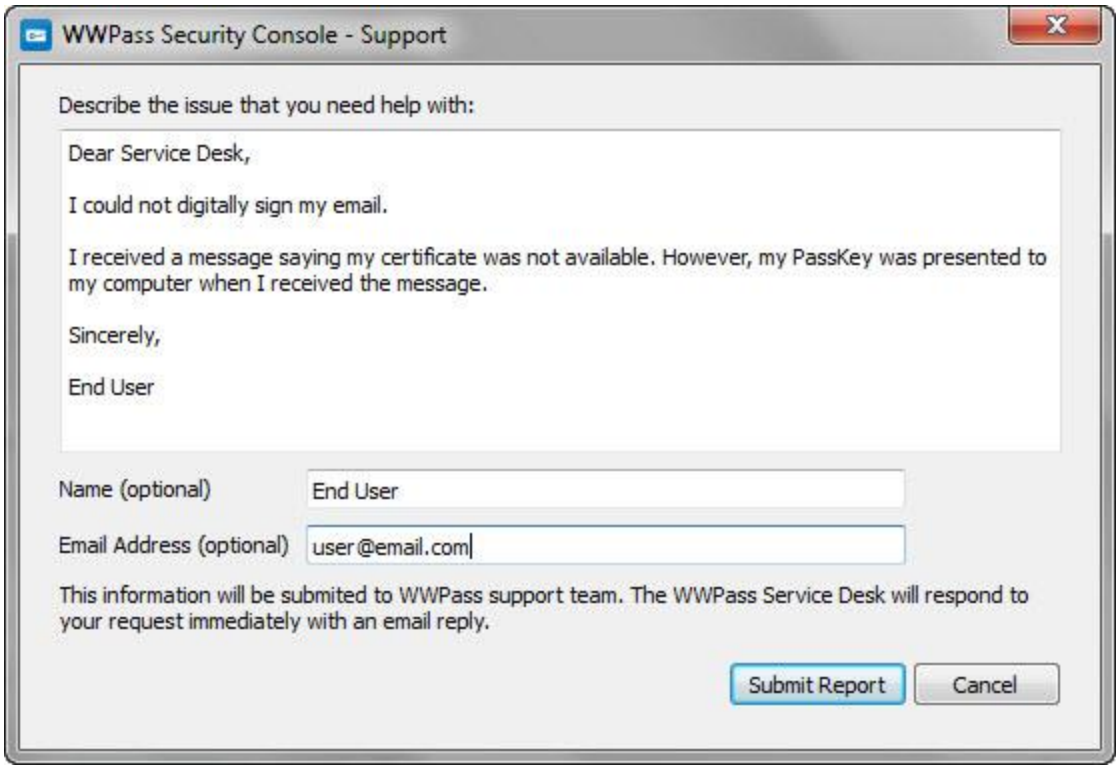
1. Select “Contact Support…” from the Dashboard Help menu.



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

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

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



CHAPTER 2 — REQUIREMENTS

System Requirements

Requirement	Details
Microsoft SharePoint Server	SharePoint Server 2010 is supported: • SharePoint should be configured for Smart Card logon and authentication via ADFS (Active Directory Federation Services) or a third-party identity management system. (PassKeys use Smart Card logon.) • Windows Server should be configured with Microsoft Internet Information Services (IIS), SQL Server, and all other required components. See Microsoft documentation for more information.
Certificate Authority	A Certificate Authority (CA) is needed to issue digital X.509 certificates for user authentication into SharePoint. 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). An Active Directory Domain Controller is used to authenticate users. (An external third-party CA such as Comodo can also be used to issue certificates.)
Internet access	Outbound TCP connections should be allowed from user computers to ports 80 (HTTP) and 443 (HTTPS). Network software and hardware (including routers and firewalls) should not block connections to these ports.

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:** Outbound TCP connections must be allowed to ports 80 (HTTP) and 443 (HTTPS).
User accounts	A Windows domain account is needed. In addition: • **Active Directory account:** You and your computer should be members of the Active Directory domain and part of the correct group. • **SharePoint account:** Your Active Directory account must be a member of a SharePoint group.
Web browser	This is needed to access SharePoint, activate your KeySet, and authenticate with your PassKey. You might also need a browser to download a certificate from a third-party CA such as Comodo. The following browsers are supported: • Microsoft Internet Explorer 8 and later (32-bit and 64-bit) • Chrome 20 and later • Mozilla Firefox 14 and later • Opera 11 and later
Certificate for SharePoint	This is 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 into SharePoint with a PassKey.
WWPass KeySet	This includes the PassKey used for logging into SharePoint.
WWPass Security Pack	This includes software that is needed to activate your KeySet and use WWPass Security for SharePoint. To obtain the software pack, contact a system administrator at your organization or Sales at WWPass: 1-888-997-2771

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 into SharePoint using a PassKey.

For complete information on SharePoint 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 SharePoint users. Certificates are associated with user PassKeys and used for authenticating into SharePoint.

2. Make sure Microsoft Internet Information Services (IIS) uses Windows authentication:

   a) Log in to Server Manager.

   b) Expand Roles and Web Server (IIS) in left panel.

   c) Left-click Internet Information Services (IIS) Manager.

   d) In Connections panel, expand nodes for SharePoint host, Sites, and SharePoint site.

   e) Double-click Authentication icon in IIS section in right pane. Windows authentication should be enabled.)

3. Set up a PassKey for your own use:

   a) Install the latest WWPass Security Pack on your computer.

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

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

Prepare to Issue Certificates from a CA

This topic provides guidelines to set up issuance of digital X.509 certificates from an internal Certificate Authority (CA). These 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 the Active Directory Certificate Services (included with the server.)

An Active Directory Domain Controller is used for user authentication.

For more information, see Microsoft's documentation.

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

Guidelines

1. Select the Active Directory Certificate Services role from the Server Manager when configuring the Certificate Authority on a Windows Server. Select the following role services as well:
   - Certification Authority (issues certificates).
   - Certification Authority Web Enrollment (provides the Active Directory web interface for certificate enrollment).

2. Configure the Smart Card Logon 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 Logon as the Certificate Template in Certificate Services when they request a certificate.

3. On 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.

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 into SharePoint using a PassKey.

Topics In This Chapter

- Smart Start for Users
- Obtain a Certificate

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.
2. Obtain and activate a WWPass KeySet, which includes a PassKey. (If you are currently using another WWPass solution, your KeySet is already activated.)
3. Obtain a certificate for SharePoint and associate it with your PassKey. Connect your PassKey to your computer before you begin.

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 into SharePoint. It is stored in the WWPass secure cloud storage, where it cannot be stolen.

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.

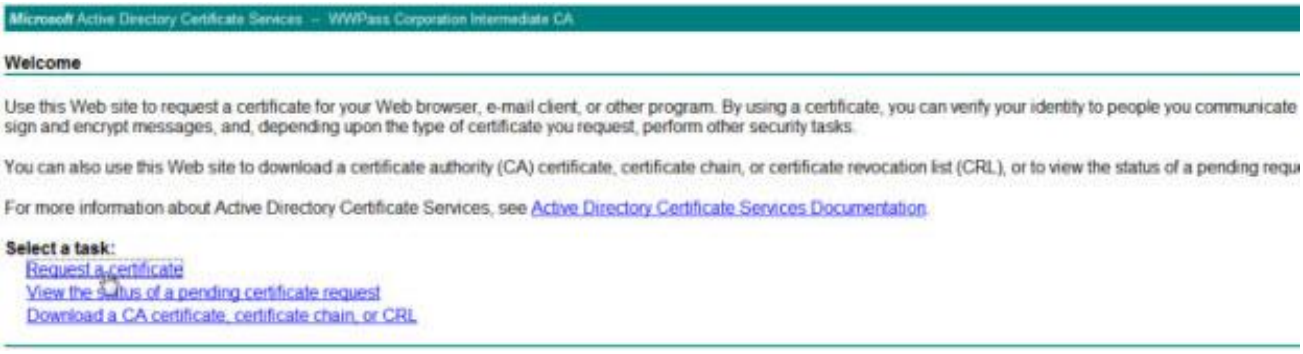
If your certificate is available in a file formt, you can import it to your PassKey using the WWPass Dashboard, which is installed as part of WWPass Security Pack.

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. Connect your PassKey to your computer. This will ensure your certificate is associated with your PassKey.
2. Open the Internet Explorer web browser on 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**.

The Options dialog is displayed.

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

   a) Select the **WWPass 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 PIN prompt that appears:

   - If certificate requests are automatically approved, your certificate is associated with your PassKey right away. You can now use it to log into SharePoint. Your set up is now complete.
   - If certificate requests are explicitly approved, the Certificate Pending page appears with your Request ID and instructions on retrieving certificates. When your certificate is ready, continue the process at the next step.

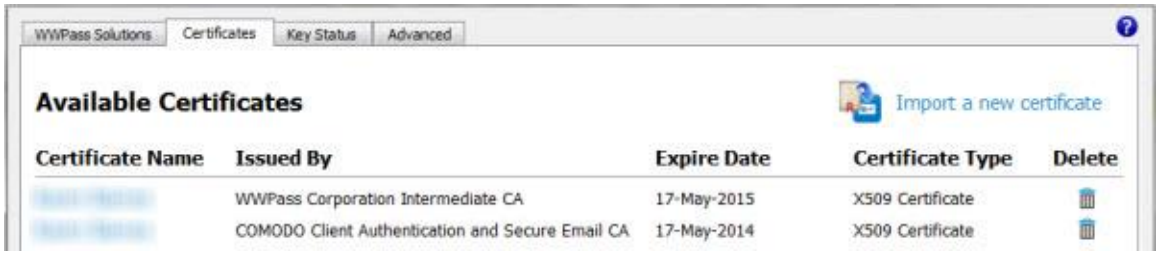
6. Return to Active Directory Certificate Services to check the status of your request. Click **View the status of a pending certificate request**.

7. Next click the date (of the request) link to retrieve the certificate.

8. When "Certificate Issued" is shown as the status, click **Install this certificate**. Then enter the PIN (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 into SharePoint.

To import a certificate using WWPass Dashboard

1. Connect your PassKey to your computer. This ensures that the certificate is associated with your PassKey.
2. Open WWPass Dashboard. Dashboard is identified by the WWPass Key icon in your 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.

CHAPTER 5 — USE YOUR PASSKEY TO LOG IN

This chapter covers using a PassKey to log into SharePoint.

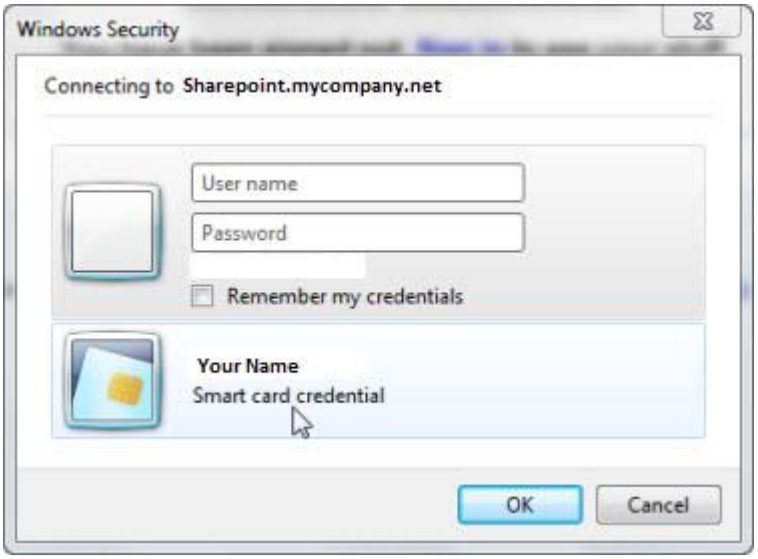
Topics In This Chapter

Log into SharePoint Using a PassKey

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

To log into SharePoint using your PassKey

1. Go to your SharePoint site using Internet Explorer.
2. Connect your PassKey to your computer.
3. When prompted to connect to SharePoint, click your name (shown above Smart Card credential). A field for a PIN appears.



4. Enter the access code for your PassKey in the PIN field and click OK. Your SharePoint home page appears.