



# **USER GUIDE**

## **WWPass Security for SharePoint**

**For WWPass Security Pack 2.6**

May 2014

## TABLE OF CONTENTS

CHAPTER 1 — Welcome .....	3
Introducing WWPASS Security for SharePoint .....	4
Related Documentation .....	5
Presenting Your PassKey to Your Computer .....	6
Need Assistance? .....	7
Report a Problem from Dashboard .....	7
CHAPTER 2 — Requirements .....	8
System Requirements .....	8
User Requirements .....	9
Chapter 3 — Setup for Administrators .....	10
Smart Start for Administrators .....	11
Prepare to Issue Certificates from a CA .....	12
Guidelines .....	12
Chapter 4 — Setup for Users .....	13
Smart Start for Users .....	14
Obtain a Certificate .....	14
Chapter 5 — Use Your PassKey to Log In .....	18
Log Into SharePoint Using a PassKey .....	19

## CHAPTER 1 — WELCOME

---

This chapter introduces WWPass® Security for SharePoint™ and provides information on using a PassKey™ from WWPass, accessing related documentation, and contacting WWPass Product Support.

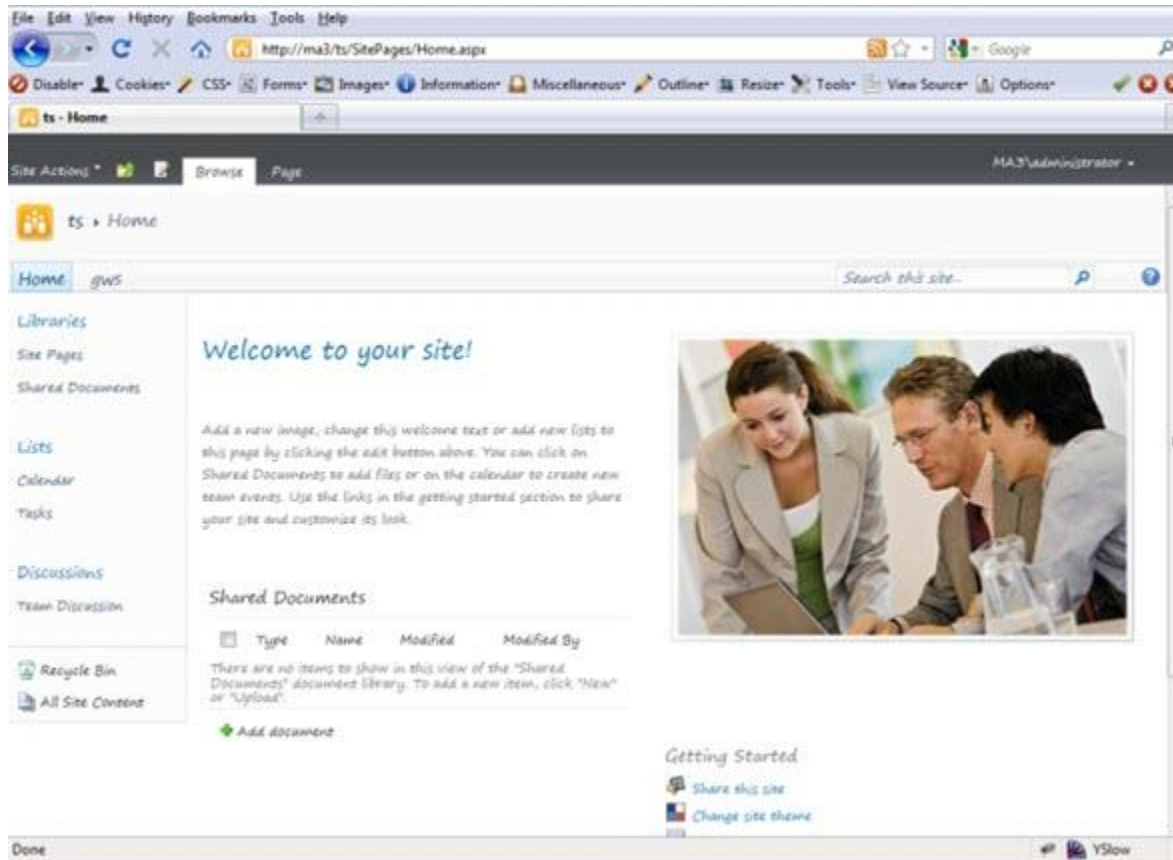
### Topics In This Chapter

---

- [Introducing WWPass Security for SharePoint](#)
- [Related Documentation](#)
- [Presenting Your PassKey to Your Computer](#)
- [Need Assistance?](#)

## Introducing WWPass Security for SharePoint

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



WWPass Security for SharePoint allows you to log into SharePoint from a web browser using a PassKey instead of a username and password. You can then access all content you have permissions for in SharePoint.

PassKey authentication can be easily integrated into SharePoint implementations that use Smart Card logon and certificates.

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

**Note:** WWPass Security for SharePoint 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. Click [here](#) to access documentation for the Security Pack.

## Related Documentation

This documentation provides information on WWPass Security for SharePoint 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	<a href="#">HTML</a>	<a href="#">PDF</a>
WWPass Security Pack		
Installation		
Windows	<a href="#">HTML</a>	<a href="#">PDF</a>
Mac	<a href="#">HTML</a>	<a href="#">PDF</a>
Linux	<a href="#">HTML</a>	<a href="#">PDF</a>
WWPass Dashboard for Security Pack	<a href="#">HTML</a>	<a href="#">PDF</a>
WWPass Solutions for Security Pack		
WWPass BlackBook	<a href="#">HTML</a>	
WWPass Security for Email (Outlook & OWA)	<a href="#">HTML</a>	<a href="#">PDF</a>
Security for Email (Thunderbird)	<a href="#">HTML</a>	<a href="#">PDF</a>
WWPass Security for VPN (Juniper VPN)	<a href="#">HTML</a>	<a href="#">PDF</a>
Security for VPN (OpenVPN)	<a href="#">HTML</a>	<a href="#">PDF</a>
WWPass Security for Windows Logon	<a href="#">HTML</a>	<a href="#">PDF</a>
WWPass Security for SharePoint	<a href="#">HTML</a>	Currently open
Personal Secure Storage		
Windows		<a href="#">PDF</a>
Mac		<a href="#">PDF</a>
Linux		<a href="#">PDF</a>

## **Presenting Your PassKey to Your Computer**

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

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

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

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

You are given three chances to enter the correct code. If you enter the wrong access code three times in 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 as follows:

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

Email [support@wwpass.com](mailto: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, which is included in the WWPass Security Pack.

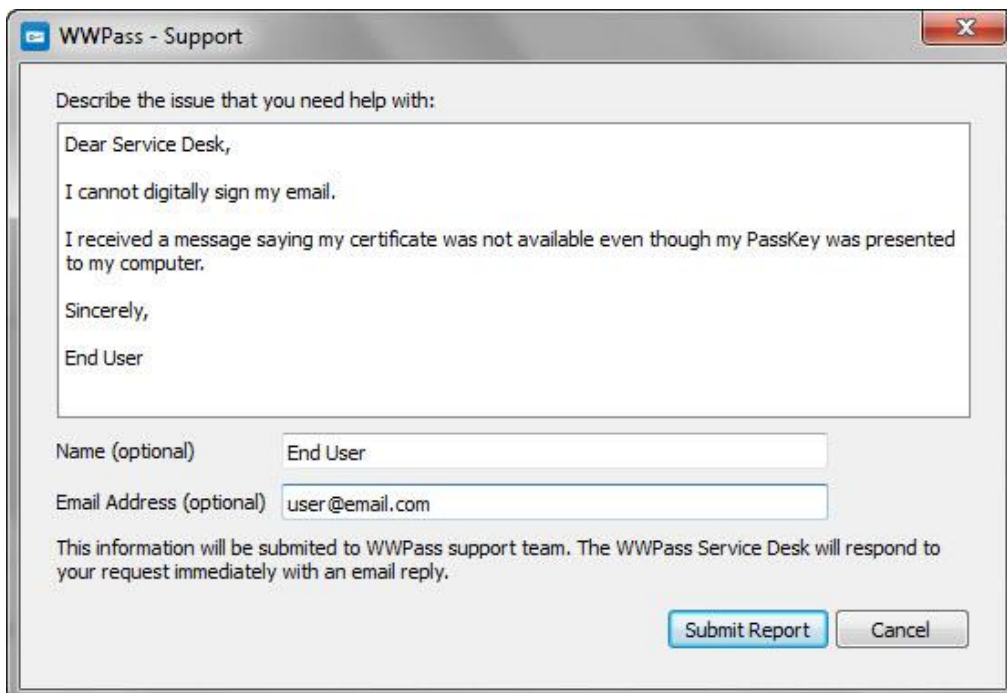
The email identifies version numbers for your Security Pack and operating system. In addition, current logs for WWPass software are automatically attached to the email.

Logs contain information that can help Product Support troubleshoot any problem you experience. For example, logs contain information such as actions and their times, and services accessed.

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  to send your report along with the current version of all available logs.



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

Describe the issue that you need help with:

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

Name (optional)

Email Address (optional)

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

## CHAPTER 2 — REQUIREMENTS

### System Requirements

Requirement	Details
<b>Microsoft SharePoint Server</b>	SharePoint Server 2010 is supported: <ul style="list-style-type: none"><li>• 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.)</li><li>• Windows Server should be configured with Microsoft Internet Information Services (IIS), SQL Server, and all other required components. See Microsoft documentation for more information.</li></ul>
<b>Certificate Authority</b>	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 <a href="#">Comodo</a> can also be used to issue certificates.)
<b>Internet access</b>	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
<b>Computer with Windows operating system</b>	<p>The following versions of Microsoft Windows are supported:</p> <ul style="list-style-type: none"> <li>• Windows 8.1 (32-bit and 64-bit)</li> <li>• Windows 8 (32-bit and 64-bit)</li> <li>• Windows 7 (32-bit and 64-bit)</li> </ul> <p><b>Note:</b> Outbound TCP connections must be allowed to ports 80 (HTTP) and 443 (HTTPS).</p>
<b>User accounts</b>	<p>A Windows domain account is needed. In addition:</p> <ul style="list-style-type: none"> <li>• <b>Active Directory account:</b> You and your computer should be members of the Active Directory domain and part of the correct group.</li> <li>• <b>SharePoint account:</b> Your Active Directory account must be a member of a SharePoint group.</li> </ul>
<b>Web browser</b>	<p>The following web browsers are supported:</p> <ul style="list-style-type: none"> <li>• Internet Explorer 8 and later (32-bit and 64-bit)</li> <li>• Chrome 20 and later</li> <li>• Firefox 14 and later</li> <li>• Opera 11 and later</li> </ul>
<b>Certificate for SharePoint</b>	<p>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.</p>
<b>WWPass KeySet</b>	<p>This includes the PassKey used for logging into SharePoint. Click <a href="#">here</a> to open KeySet help.</p>
<b>WWPass Security Pack</b>	<p>This includes software that is needed to activate your KeySet and use WWPass Security for SharePoint. Click <a href="#">here</a> to open Security Pack help.</p>

## 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](#)
- [Prepare to Issue Certificates from a CA](#)

## 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 WWPASS Security Pack on your computer. Click [here](#) for Security Pack help.
  - b) Obtain and activate a WWPASS KeySet. This includes a PassKey. (If you are currently using another WWPASS solution, your KeySet is already activated.) Click [here](#) for KeySet help.
  - 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 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 issue certificates using 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 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. 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.

## 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 the 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 SharePoint and associate it with your PassKey (see below). Present 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 WWPass secure cloud storage, where it cannot be stolen. Click [here](#) for more information.

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.

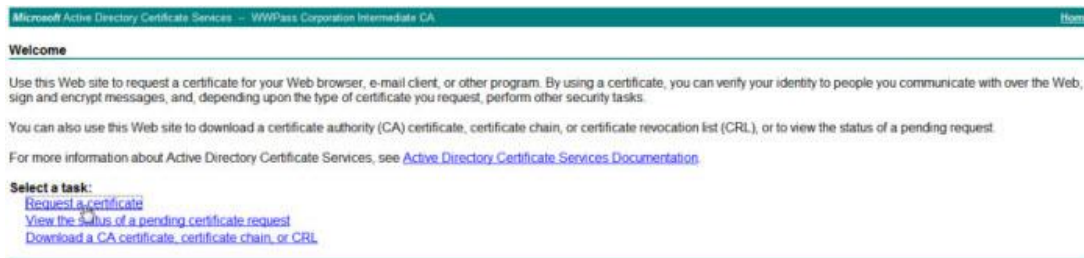
 **Note:** If the Certificate Authority's root certificate for your domain is not trusted by your computer, Active Directory Certificate Services displays a message that says your root CA is not trusted. Click the link provided to install the root CA on your computer.

### To obtain a certificate via Active Directory

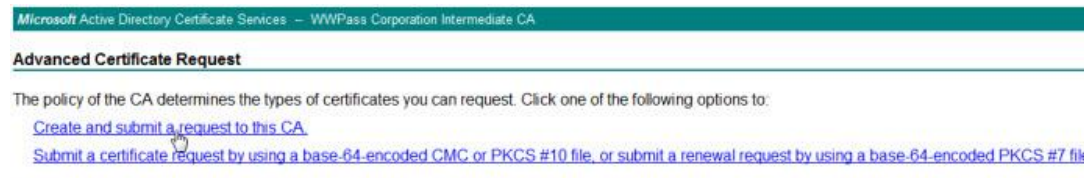
---

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>

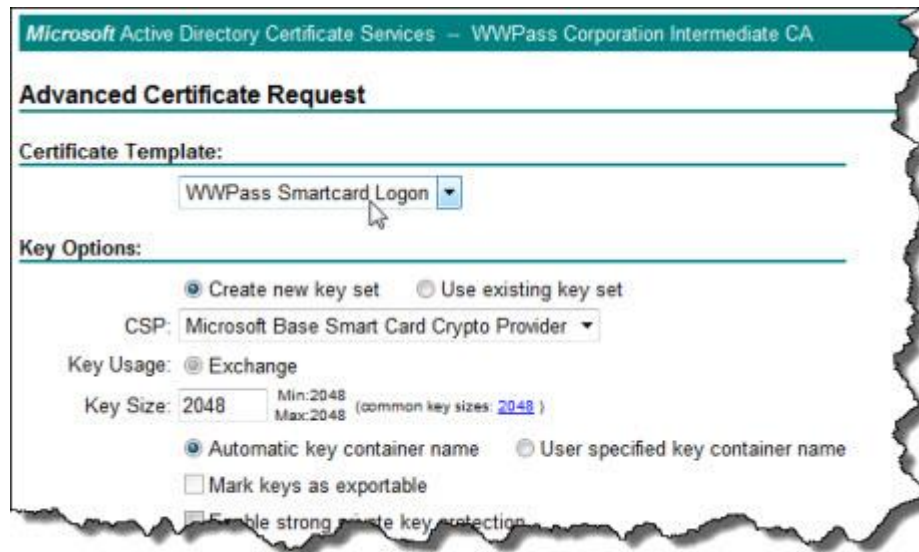
- From the CA Welcome page, click **Request a certificate**.



- 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 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.
  - If certificate requests are explicitly approved, the Certificate Pending page appears with your Request ID and instructions on retrieving certificates. 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.





- 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.

Microsoft Active Directory Certificate Services – WWPass Corporation Intermediate CA



### Certificate Issued

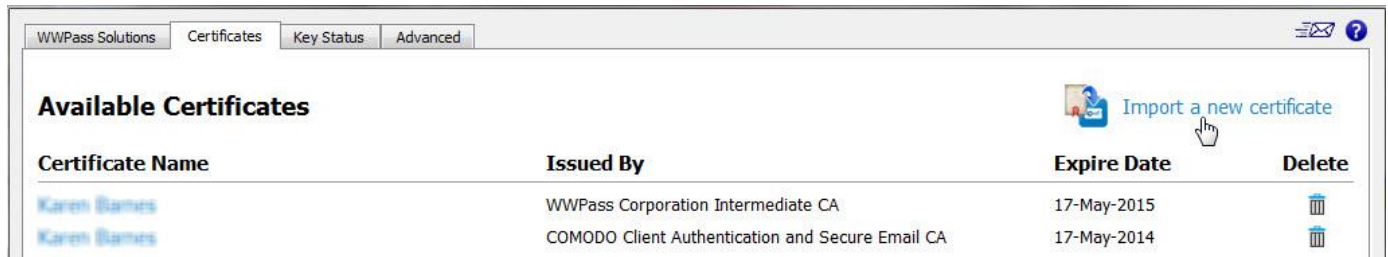
The certificate you requested was issued to you.

 [Install this certificate](#)

Save response


## To import a certificate using the WWPass Dashboard

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



WWPass Solutions Certificates Key Status Advanced

**Available Certificates** [Import a new certificate](#)

Certificate Name	Issued By	Expire Date	Delete
<a href="#">Karen Barnes</a>	WWPass Corporation Intermediate CA	17-May-2015	
<a href="#">Karen Barnes</a>	COMODO Client Authentication and Secure Email CA	17-May-2014	

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

## CHAPTER 5 — USE YOUR PASKEY TO LOG IN

---

This chapter covers using a PassKey to log into SharePoint.

### Topics In This Chapter

---

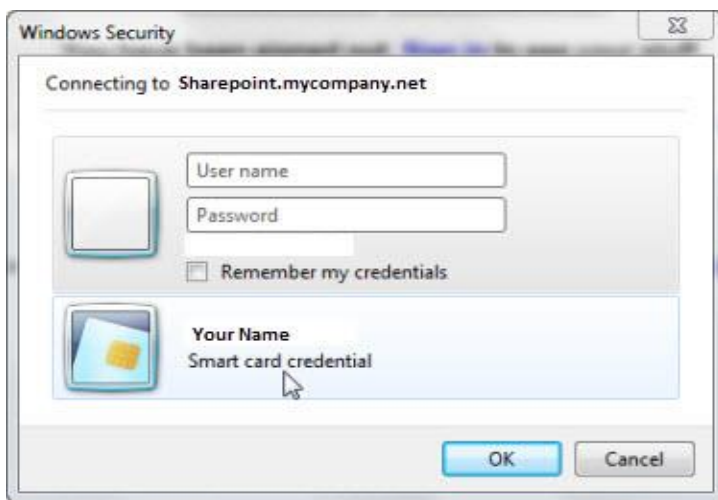
- [Log Into SharePoint Using a PassKey](#)

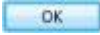
## Log Into SharePoint Using a PassKey

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 from Internet Explorer.
2. [Present](#) 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 . Your SharePoint home page appears.



