



# **USER GUIDE**

## **WWPass Security for Email (Outlook)**

**For WWPass Security Pack 2.4**

March 2014

# TABLE OF CONTENTS

Chapter 1 — Welcome .....	4
Introducing WWPass Security for Email (Outlook) .....	5
Supported Outlook Products .....	5
Related Documentation.....	6
Presenting Your PassKey to Your Computer.....	7
Need Assistance? .....	8
Report a Problem from Dashboard .....	8
Chapter 2 — Requirements .....	9
System Requirements for Outlook and OWA .....	9
User Requirements for Outlook and OWA.....	10
Chapter 3 — Setup for Administrators .....	11
Smart Start for Administrators.....	12
Prepare to Issue Certificates from a CA .....	13
CA for OWA Login.....	13
CA for Secure Email.....	13
Set Up for Certificate Enrollment with an Internal CA .....	13
Guidelines .....	14
Enable Certificate Authentication into OWA .....	15
Enable Certificate Authentication into ECP.....	17
Set Up for Certificate Selection in OWA .....	20
Chapter 4 — Setup for Users.....	22
Smart Start for Users .....	23
Obtain a Certificate .....	24
Important guidelines.....	24
Obtain a Certificate from a Third Party via Outlook .....	25
Obtain a Certificate from Your Organization Via Active Directory .....	26
Import a Certificate Using the WWPass Dashboard.....	28
Select Certificates for Outlook.....	29
Install the S/MIME Control for OWA .....	31
Select Certificates for OWA .....	33
Share Public Keys for Exchanging Secure Email .....	36
Chapter 5 — Using a PassKey with Outlook .....	37
Overview for Using a PassKey with Outlook.....	38
Use a PassKey for Digital Signing in Outlook.....	38
Use a PassKey for Encrypted Email in Outlook.....	40
Basics for encrypted messages .....	41

Chapter 6 — Using a PassKey with OWA .....	42
Overview for Using a PassKey with OWA .....	43
Before you begin .....	43
Use a PassKey for Logging into OWA .....	43
Use a PassKey for Logging into ECP .....	44
Use a PassKey for Digital Signing in OWA.....	45
Use a PassKey for Encrypted Email in OWA.....	46
Basics for encrypted messages .....	46

## CHAPTER 1 — WELCOME

---

This chapter introduces WWPass® Security for Email (Outlook)™ 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 Email \(Outlook\)](#)
- [Supported Outlook Products](#)
- [Related Documentation](#)
- [Presenting Your PassKey to Your Computer](#)
- [Need Assistance?](#)

## Introducing WWPass Security for Email (Outlook)

This documentation covers how to set up and use WWPass Security for Email (Outlook), the WWPass authentication solution for Microsoft Outlook and Outlook Web App (OWA).

Once WWPass Security for Email (Outlook) is set up, you can use a PassKey instead of a username and password in order to prove your identity when you:

- Send digitally signed email messages from Outlook or OWA.
- View encrypted messages and attachments in Outlook or OWA.
- Log in to OWA and its Exchange Control Panel (ECP).

Digitally signing email assures recipients that it's really from you. Encrypting email ensures only you and your correspondents can read it.

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



**Note:** WWPass Security for Email (Outlook) 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.

## Supported Outlook Products

WWPass Security for Email (Outlook) works with two Outlook products—Microsoft Outlook and Outlook Web App (OWA):

- **Microsoft Outlook** is a Windows application that can be used to access email on Microsoft Exchange Server or another email server. Outlook is included with Microsoft Office. Outlook versions 2010 and 2013 are supported.
- **OWA** is a webmail service that can be used to access email on Microsoft Exchange Server via a Web browser (Internet Explorer is recommended). OWA is included with Exchange Server 2010 along with Exchange Control Panel (ECP), an application that allows administrators to manage OWA accounts from anywhere via a web browser. (Outlook Web App's predecessor was called Outlook Web Access.)

## Related Documentation

This documentation provides information on WWPass Security for Email (Outlook) 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 Security for Email (Outlook & OWA)	<a href="#">HTML</a>	Currently open
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>	<a href="#">PDF</a>
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, included in the WWPass Security Pack.

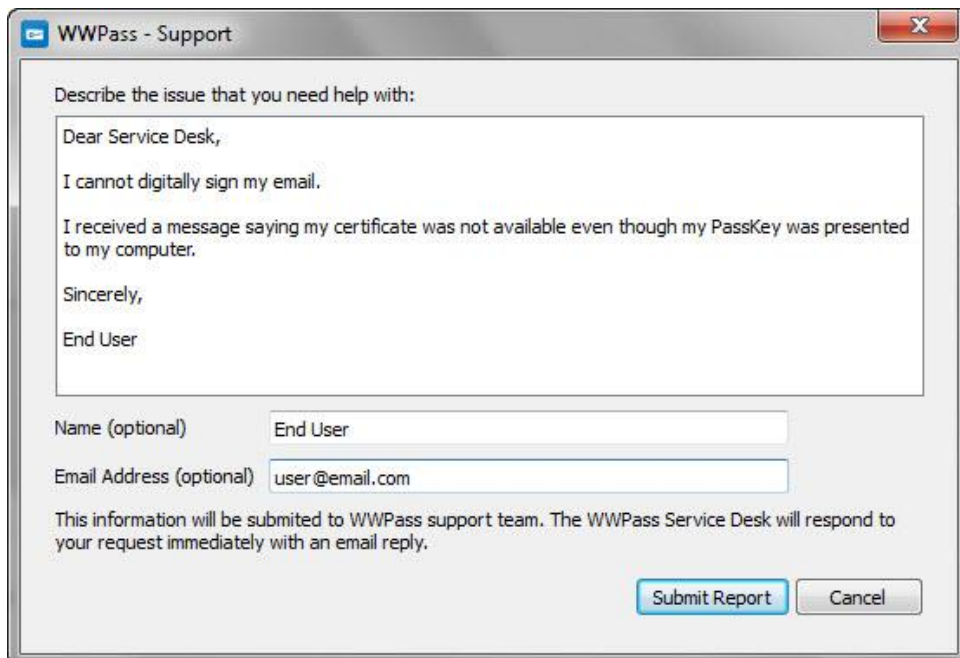
The email automatically identifies version numbers for your Security Pack and operating system. In addition, current logs for WWPass software are automatically attached to the email.

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 window titled "WWPass - Support". Inside, there is a text area for describing the issue, a "Name (optional)" field, and an "Email Address (optional)" field. The text area contains the following text:

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) End User

Email Address (optional) user@email.com

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

At the bottom right, there are two buttons: "Submit Report" and "Cancel".



## CHAPTER 2 — REQUIREMENTS

### System Requirements for Outlook and OWA

Requirement	Details
Microsoft Exchange Server	<p>An email server is required for both Outlook and Outlook Web App (OWA). Microsoft Exchange Server 2010 is supported:</p> <ul style="list-style-type: none"><li>• <b>Outlook</b>—Using Exchange is optional for Outlook. Any email server compatible with Outlook can be used.</li><li>• <b>OWA</b>—Exchange is required for OWA, which is only available with Exchange 2010.</li></ul>
Internet access	<p>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 connections to these ports.</p>
Certificate Authority	<p>A Certificate Authority (CA) is required for issuing digital X.509 certificates to users. Certificates are associated with user PassKeys and are needed to authenticate users when they use secure email features or log into OWA:</p> <ul style="list-style-type: none"><li>• <b>For login</b>—The certificate for logging into OWA must be a domain-based certificate issued by an internal CA such as the Microsoft Enterprise CA. It can be the certificate used for logging into your Windows domain if your Exchange server is on that domain. (To use the Microsoft CA, you need Active Directory Certificate Services, which is included with Windows Server; Windows Server 2008 and 2008 R2 are supported.)</li><li>• <b>For email</b>—The certificate for secure email can be issued by an internal CA or an external, third-party CA such as Comodo. The same certificate can be used for Outlook and OWA. If certificates should be trusted by email recipients outside your organization, the certificates should be issued by a widely-trusted third party. Certificates issued by an internal CA are only trusted within your organization.</li></ul> <p>If your organization uses two certificates for OWA—one for login and one for secure email, both an internal CA and an external CA are needed.</p>

## User Requirements for Outlook and OWA

Requirement	Details
Email client and account	Microsoft Outlook versions 2010 and 2013 are supported. Outlook must be installed on your computer. Outlook Web App (OWA) is included with your organization's Microsoft Exchange Server and accessed from the server via a web browser.
Computer with Windows operating system	<p>The following versions of Windows are supported:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows 8.1 (32-bit and 64-bit)</li> <li>• Microsoft Windows 8 (32-bit and 64-bit)</li> <li>• Microsoft 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>
S/MIME control	This is needed for OWA's encryption and digital signing functions. It can be <a href="#">installed</a> from OWA. (S/MIME control is not needed for Outlook.)
Certificates	<p>An X.509 certificate from a Certificate Authority (CA) is needed to authenticate your identity when you use a WWPass PassKey to:</p> <ul style="list-style-type: none"> <li>• Digitally sign or decrypt email. If the certificate for secure email is from your organization's internal CA, it is trusted only within your organization. If it is from a third-party CA, it is trusted within and outside your organization. The same certificate can be used for both Outlook and OWA.</li> <li>• Log into OWA. The certificate for login must be from your organization's internal CA.</li> </ul> <p>Ask a system administrator how to <a href="#">obtain</a> certificates.</p>
Web browser	<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> <p><b>Note:</b> Internet Explorer is recommended for OWA. It provides access to all OWA features and the S/MIME Control. The <b>Run ActiveX controls and plug-ins</b> setting should be enabled in Internet Options &gt; Security Settings.</p>
WWPass KeySet	This includes the PassKey used for authentication. Click <a href="#">here</a> to open KeySet help.
WWPass Security Pack	This includes software that is needed to activate a KeySet and use WWPass Security for Email (Outlook). Click <a href="#">here</a> 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 authenticate with a PassKey in Outlook and OWA.

For complete information on authentication for Outlook and OWA, see Microsoft documentation.

### Topics In This Chapter

---

- [Smart Start for Administrators](#)
- [Set Up for Certificate Enrollment](#)
- [Enable Certificate Enrollment into OWA](#)
- [Enable Certificate Enrollment into ECP](#)
- [Set Up for Certificate Selection in OWA](#)

## 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. Set up Microsoft Exchange Server according to Microsoft documentation and requirements. Exchange should be configured with Microsoft Internet Information Services (IIS). If you are using another email server, follow documentation for that server.
2. Prepare to issue certificates from a Certificate Authority (CA) for Outlook and/or OWA users. If your organization uses two certificates for OWA (one for login and one for secure email), both an internal CA and an external CA are needed.
3. Enable certificate authentication as follows:
  - [Enable](#) certificate authentication into OWA for end users.
  - [Enable](#) certificate authentication into ECP (Exchange Control Panel) for administrators. This allows you to log in to the Exchange Control Panel and manage the Exchange server from anywhere.
4. If your organization uses two certificates for OWA (one for login and one for secure email), [set up](#) for certificate selection by OWA users. This allows them to select a widely-trusted third party certificate for digital signing.



**Note:** If you do not set up for certificate selection, the certificate for login is used for digital signing. However, the login certificate will not be trusted by email recipients outside your organization.

5. 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. Click [here](#) for KeySet help. (If you are currently using another WWPass solution, your KeySet is already activated.)
  - c) [Obtain](#) an email certificate and associate it with your PassKey. [Present](#) your PassKey to your computer before you begin.



**Tip:** To make it easy for users to exchange encrypted email, create a Global Address List on the Exchange Server. Each user's public key is available in the list. This allows users to send encrypted email to others on the list. It also lets them decrypt email from others on the list. If you do not create a Global Address List, users must share their public keys individually.

## Prepare to Issue Certificates from a CA

In order to issue X.509 certificates for authenticating users with Outlook and/or OWA, a Certificate Authority (CA) must be available. If your organization uses two certificates for OWA (one for login and one for secure email), both an internal CA and an external CA are needed.

### CA for OWA Login

The certificate for logging into OWA must be a domain-based certificate issued by an internal CA such as the Microsoft Enterprise CA. Click [here](#) for guidelines on using an internal CA.

If users already have certificates for logging into your Windows domain, the certificates can be used for OWA login as long as your Exchange server is on the Windows domain. In this case, certificates are exported to user PassKeys (which use Smart Card technology). Click [here](#) for information from Microsoft's TechNet site.

### CA for Secure Email

The certificate for secure email can be issued by an internal CA or an external, third-party CA such as Comodo.

The same certificate can be used for both email clients. Also, the login certificate for OWA can be used for secure email.

However, if you want a certificate to be trusted by email recipients outside your organization, it should be issued by a widely-trusted third party. Certificates issued by an internal CA are only trusted within your organization.

See Microsoft documentation for information on using an external, third-party CA. For example, see [Guidelines for Enabling Smart Card Logon with Third-party Certification Authorities](#) and [Requirements for Domain Controller Certificates from a Third-Party CA](#) on Microsoft's Support site.



**Note:** A third-party root CA must be added to trusted roots in an Active Directory Group Policy object and the third-party issuing the CA must be added to the NTAuth store in Active Directory. (Microsoft Enterprise CAs are added to the NTAuth store by default.)

## Set Up for Certificate Enrollment with an Internal CA

This topic provides guidelines on setting up to issue domain-based certificates from an internal Certificate Authority (CA)—a Microsoft CA server on your Windows domain. The certificates are self-signed by your organization and trusted within your organization (but not outside).

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

An Active Directory Domain Controller is used for user authentication.

For complete information, see Microsoft documentation.



**Note:** To use the Microsoft CA, you need Active Directory Certificate Services, which is included with Windows Server; Windows Server 2008 and 2008 R2 are supported.

## 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 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.



## Enable Certificate Authentication into OWA

Follow the steps below to enable certificate authentication into OWA (Outlook Web App). This allows users to log into OWA with their PassKeys. Important steps are to:

- Set the authentication method for the OWA virtual directory on the Exchange server.
- Turn off forms-based authentication
- Set Windows Authentication and Basic Authentication to false.



**Note:** OWA and ECP should use the same authentication method. See [Enable Certificate Authentication into ECP](#).

### To enable certificate authentication into OWA

#### 1. Install the certificate-based authentication feature

Install the certificate-based authentication feature as follows:

- a) Start the Windows PowerShell console with the **Run as administrator** option.
- b) Run the following commands:

```
Import-Module ServerManager  
  
Add-WindowsFeature web-client-auth
```

#### 2. Enable certificate authentication

Enable certificate authentication as follows:

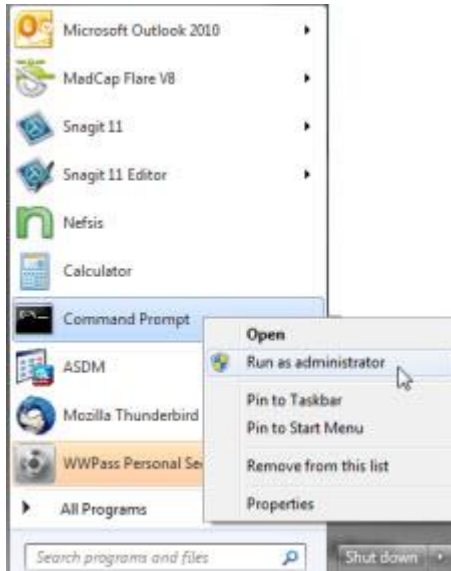
- a) Log in to Exchange and open Server Manager.
- b) From the left pane, expand **Roles** and **Web Server (IIS)**. Then left-click **Internet Information Services (IIS) Manager**.
- c) From the Connections pane, highlight the name of your Exchange server. The Home pane for your server is displayed.
- d) Double-click the Authentication icon in the Home pane. The Authentication pane is displayed.
- e) Right-click **Active Directory Client Certificate Authentication** in the Authentication pane and select **Enable** in the Actions pane on the right.
- f) Return to the left pane and expand **Web Server (IIS)**. Then left-click **Internet Information Services (IIS) Manager**.
- g) From the Connections pane, expand **Sites** and **Default Web Site**. Then select the OWA virtual directory. The OWA Home pane is displayed.
- h) Double-click the SSL Settings icon in the Home pane. The SSL Settings pane is displayed.
- i) Under Client Certificates, select the **Require** button.
- j) Click **Apply** in the Actions pane on the right.



### 3. Unlock the IIS feature

Unlock the IIS (Internet Information Services) feature for certificate authentication as follows:

- a) Start the Windows Command Prompt with the **Run as administrator** option.



- b) Run the following commands:

```
%windir%\system32\inetsrv\appcmd unlock config
/section:clientCertificateMappingAuthentication

%windir%\system32\inetsrv\appcmd set config "Default Web Site/OWA" -
section:clientCertificateMappingAuthentication /enabled: true
```

### 4. Configure the OWA virtual directory

Configure the OWA virtual directory from the Exchange Management Shell. This will turn off forms based authentication and set Windows Authentication and Basic Authentication to false so that users will be required to present a certificate (via their PassKey) to access OWA.

- a) Start the Exchange Management Shell with the **Run as administrator** option.

- b) Run the following commands:

```
set-owavirtualdirectory -identity "server-name\OWA (Default Web
Site)" -WindowsAuthentication:$false

set-owavirtualdirectory -identity "server-name\OWA (Default Web
Site)" -BasicAuthentication:$false

set-owavirtualdirectory -identity "server-name\OWA (Default Web
Site)" -FormsAuthentication:$false

IISreset /noforce
```



**Note:** If an error occurs when you run the first command, enter your full server name (including domain) instead of server-name. For example:

```
set-owavirtualdirectory -identity "t-exch-01-11.exch.lan\OWA (Default Web
Site)" -WindowsAuthentication:$false -BasicAuthentication:$false -
FormsAuthentication:$false
```

## Enable Certificate Authentication into ECP

Follow the steps below to enable certificate authentication into ECP (Exchange Control Panel), the web-based tool for managing OWA accounts. This allows administrators to log in to ECP with their PassKeys. Important steps are to:

- Set the authentication method for the ECP virtual directory on the Exchange server.
- Turn off forms-based authentication.
- Set Windows Authentication and Basic Authentication to false.



**Note:** ECP and OWA should use the same authentication method. For more information, see [Enable Certificate Authentication into OWA](#).

### To enable certificate authentication into ECP

#### 1. Install the certificate-based authentication feature

Install the certificate-based authentication feature as follows:

- a) Start the Windows PowerShell console with the **Run as administrator** option.
- b) Run the following commands:

```
Import-Module ServerManager  
  
Add-WindowsFeature web-client-auth
```

#### 2. Enable certificate authentication

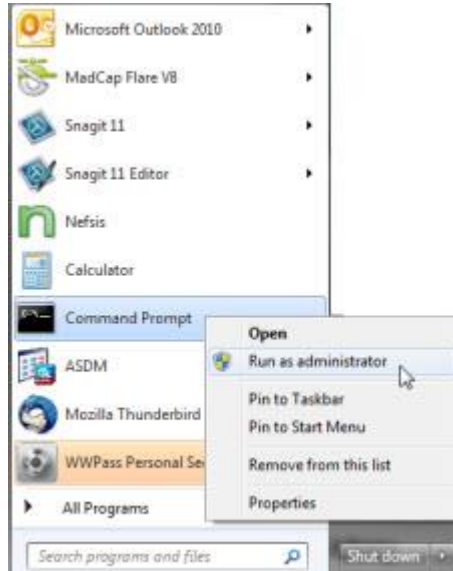
Enable certificate authentication as follows:

- a) Log in to Exchange and open Server Manager.
- b) From the left pane, expand **Roles** and **Web Server (IIS)**. Then left-click **Internet Information Services (IIS) Manager**.
- c) From the Connections pane, highlight the name of your Exchange server. The Home pane for your server is displayed.
- d) Double-click the Authentication icon in the Home pane. The Authentication pane is displayed.
- e) Right-click **Active Directory Client Certificate Authentication** in the Authentication pane and select **Enable** in the Actions pane on the right.
- f) Return to the left pane and expand **Web Server (IIS)**. Then left-click **Internet Information Services (IIS) Manager**.
- g) From the Connections pane, expand **Sites** and **Default Web Site**. Then select the ECP virtual directory. The ECP Home pane is displayed.
- h) Double-click the SSL Settings icon in the Home pane. The SSL Settings pane is displayed.
- i) Under Client Certificates, select the **Require** button.
- j) Click **Apply** in the Actions pane on the right.

### 3. Unlock the IIS feature

Unlock the IIS (Internet Information Services) feature for certificate authentication as follows:

- a) Start the Windows Command Prompt with the **Run as administrator** option.



- b) Run the following command:

```
%windir%\system32\inetsrv\ appcmd set config "Default Web Site/ECP" -  
section:clientCertificateMappingAuthentication /enabled:true
```

#### 4. Configure the ECP virtual directory

Configure the ECP virtual directory from the Exchange Management Shell. This will turn off forms based authentication and set Windows Authentication and Basic Authentication to false so that users will be required to present a certificate (via their PassKey) to access OWA.

a) Start the Exchange Management Shell with the **Run as administrator** option.

b) Run the following commands:

```
set-ecpvirtualdirectory -identity "server-name\ECP (Default Web Site)"  
-WindowsAuthentication:$false
```

```
set-ecpvirtualdirectory -identity "server-name\ECP (Default Web Site)"  
-BasicAuthentication:$false
```

```
set-ecpvirtualdirectory -identity "server-name\ECP (Default Web Site)"  
-FormsAuthentication:$false
```

```
IISreset /noforce
```



**Note:** If an error occurs when you run the first command, enter your full server name (including domain) instead of server-name. For example:

```
set-ecpvirtualdirectory -identity "t-exch-01-11.exch.lan\ECP (Default  
Web Site)" -WindowsAuthentication:$false -BasicAuthentication:$false -  
FormsAuthentication:$false
```

## Set Up for Certificate Selection in OWA

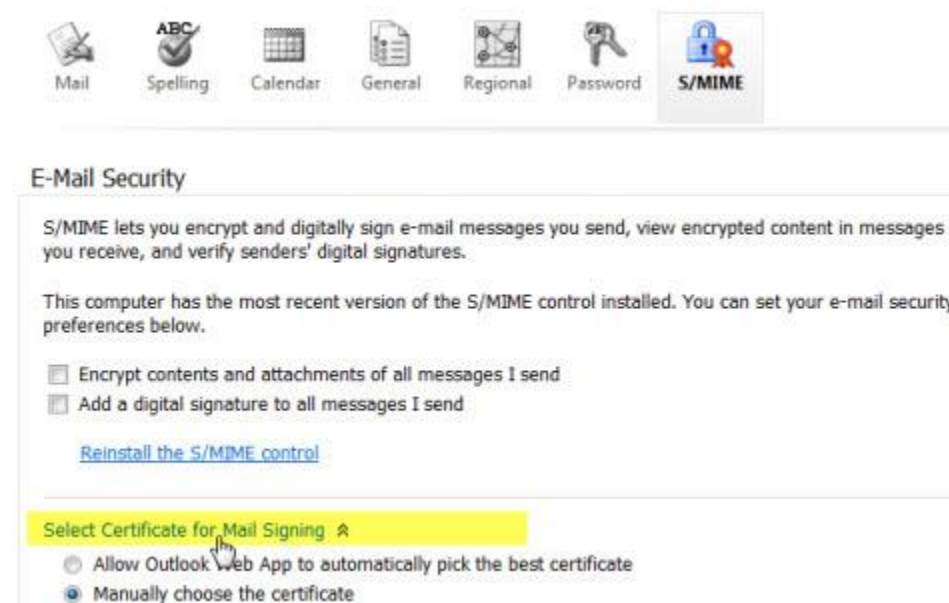
You can modify Registry keys on the Exchange server in order to:

- Allow users to select a certificate for digital signing in OWA.
- Ensure only certificates on user PassKeys can be selected.

By default, the certificate that was used for logging into OWA is also used for digital signing.

But if your organization provides different certificates for login and digital signing, you can create a Registry key that adds the Select Certificate for Mail Signing feature to E-Mail Security options in OWA's S/MIME tab.

You can also set the OnlyUseSmartCard Registry key so that only PassKey certificates are available for selection.



The Registry keys in question can be changed on a Microsoft Exchange Server that has the Client Access server role installed. Changes are made per server and take effect immediately. Users do not need to sign out or restart OWA. If you have more than one Client Access server, the changes must be made on each server.



**Important:** When you change Registry settings, you are changing a Microsoft product, not a WWPass product. According to Microsoft, serious problems might occur if you modify the registry incorrectly using Registry Editor or another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

## To set up for certificate selection in OWA

---

1. Log into your Exchange server as an Exchange Administrator.
2. Start Registry Editor (regedit) by clicking Start and Run. Then type regedit and press Enter.
3. Expand the HKLM\System\CurrentControlSet\services\MSEExchangeOWA\SMIME subkey.
4. Create the Registry key for certificate selection as follows:
  - a) Right-click the SMIME key, click New and click DWORD (32-bit).
  - b) Name the new DWORD value as follows: AllowUserChoiceOfSigningCertificate
  - c) Double-click AllowUserChoiceOfSigningCertificate and set the value to 1.
5. Set or create the Registry key to force selection of certificates on PassKeys as follows:
  - a) Find the OnlyUseSmartCard key.
  - b) Set the key value to 1.
  - c) If the key doesn't exist, create a new DWORD with the name OnlyUseSmartCard. Then set the key value to 1.
6. Close the Registry Editor.
7. Click Start and Run. Then type cmd and press Enter.
8. From the command prompt, run IISReset /noforce. Alternatively, you can restart the IIS Admin service in Services.msc.

## CHAPTER 4 — SETUP FOR USERS

---

This chapter covers setup for users. It includes information on essential tasks that must be performed before you can authenticate with a PassKey in Outlook and OWA.

### Topics In This Chapter

---

- [Smart Start for Users](#)
- [Obtain a Certificate](#)
- [Import a Certificate](#)
- [Select Certificates for Outlook](#)
- [Install the S/Mime Control for OWA](#)
- [Select Certificates for OWA](#)
- [Share Public Keys for Exchanging Secure Email](#)



## 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. Click [here](#) for Security Pack help.
2. Obtain and activate a WWPass KeySet. This includes a PassKey. Click [here](#) for KeySet help.



**Note:** If you are currently using another WWPass solution, your KeySet is already activated.

3. [Obtain](#) an email certificate and associate it with your PassKey. [Present](#) your PassKey to your computer before you begin.
4. [Install](#) the S/MIME control in OWA. Afterward, encryption and digital signing features are displayed in the OWA interface. (Skip this step for Outlook.)
5. Select an email certificate for signing and encryption in [Outlook](#) and/or [OWA](#).
6. [Share](#) public key certificates with email correspondents by sending them digitally-signed messages. This allows you to exchange encrypted email with each other.

## Obtain a Certificate

Ask a system administrator how to obtain a certificate from the Certificate Authority (CA) used by your organization:

- A common method for obtaining email certificates issued by a third-party CA is with a function in Outlook's Trust Center. Click [here](#) to see example steps.
- A common method for obtaining certificates issued by your organization's internal CA is with Active Directory Certificate Services. Click [here](#) to see example steps.

Your certificate is associated with your PassKey and serves as a credential that proves your identity when you use secure email features (digital signing and encryption) or log into OWA. The certificate is stored in WWPass secure cloud storage, where it cannot be stolen. Click [here](#) for more information.

If your organization uses different certificates for secure email and logging into OWA, two certificates must be obtained.

If your organization emails your certificate in a file, you can import the certificate for use with your PassKey using the WWPass Dashboard, which is installed as part of the WWPass Security Pack.



**Note:** If you are using both Outlook and OWA, the same certificate can be used for secure email in both applications.

## Important guidelines

Whatever method you use to obtain a certificate, follow these guidelines to ensure the certificate is associated with your PassKey:

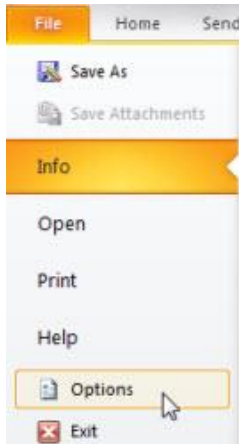
- Before you obtain a certificate, present your PassKey to your computer. To do this, insert your PassKey into a USB port on your computer or place the PassKey on an NFC reader connected to your computer.
- When you obtain a certificate, select the following as the CSP: **Microsoft Base Smart Card Crypto Provider**. (CSP stands for Cryptographic Service Provider.)

## Obtain a Certificate from a Third Party via Outlook

The steps below are an example of how to obtain a certificate issued by a third-party CA via Outlook's Trust Center. Steps at your company might be different.

### To obtain email certificate via Outlook

1. Present your PassKey to your computer by placing it on an NFC reader or inserting it into a USB port.
2. Click the File Tab in Outlook and click **Options**.



3. Click  on the right.

4. Click  under Microsoft Outlook Trust Center.

5. Click .

6. Click  on the E-mail Security tab. A Microsoft page displays a list of Certificate Authorities.

7. Click the link for the Certificate Authority your organization is using. Then follow their instructions to download the certificate. Select options as follows:

- Select "Microsoft Base Smart Card Crypto Provider" as the CSP.
- Do not select the Exportable and User Protected options.
- Use 2048 for Key Size.

8. Enter the access code for your PassKey. The email certificate is associated with your PassKey.



## Obtain a Certificate from Your Organization Via Active Directory

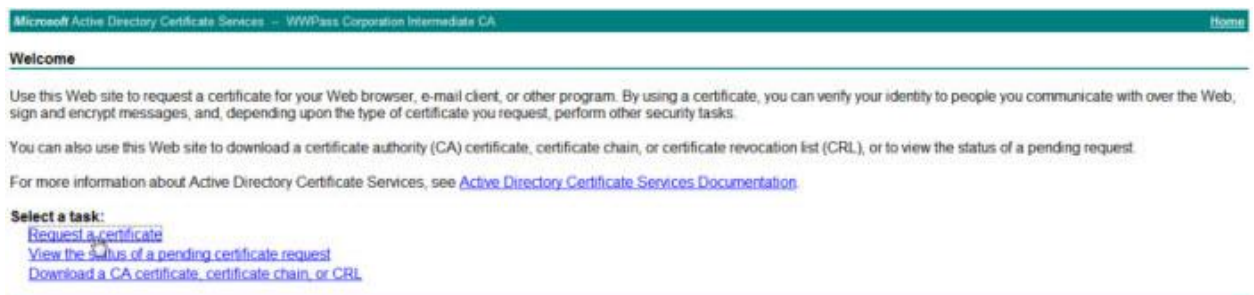
The steps below are an example of how to obtain a certificate issued by your organization's internal CA via Active Directory Certificate Services. Steps at your company might be different.



**Note:** If the "root certificate" for your Juniper VPN is not trusted by your computer, Active Directory indicates this and provides a link that lets you install the root CA on your computer.

### To obtain a certificate via Active Directory

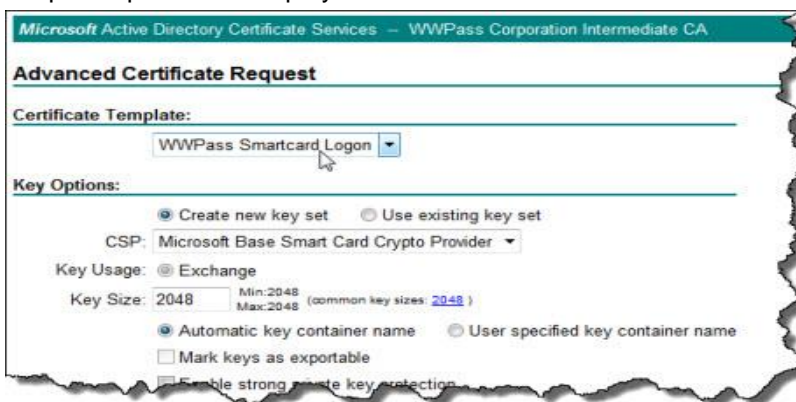
1. Present your PassKey to your computer by placing it on an NFC reader or inserting it into a USB port. This ensures your certificate is associated with your Passkey.
2. Open Internet Explorer from your computer and go to Active Directory using the URL provided by a system administrator, for example: <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**.



Request 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.

**Key Options:**

☒ Create new key set    ☐ Use existing key set

CSP: **Microsoft Base Smart Card Crypto Provider**

- 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 access code for your PassKey in the prompt that appears:
  - If certificate requests are automatically approved, your certificate is associated with your PassKey. You can now use it for authentication with Outlook and OWA.
  - If certificate requests are explicitly approved, the Certificate Pending page appears with your Request ID and instructions. Go to the next step.

Microsoft Active Directory Certificate Services -- WWPass Corporation Intermediate CA

**Certificate Pending**

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 839.

Please return to this web site in a day or two to retrieve your certificate.

**Note:** You must return with this web browser within 10 days to retrieve your certificate

6. Go to Active Directory to check the status of your request. Use the URL provided by an administrator. First click **View the status of a pending certificate request**.

Microsoft Active Directory Certificate Services -- WWPass Corporation Intermediate CA [Home](#)

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

[Request a certificate](#)  
[View the status of a pending certificate request](#)  
[Download a CA certificate, certificate chain, or CRL](#)

Next click the date link for the certificate.

Microsoft Active Directory Certificate Services -- WWPass Corporation Intermediate CA

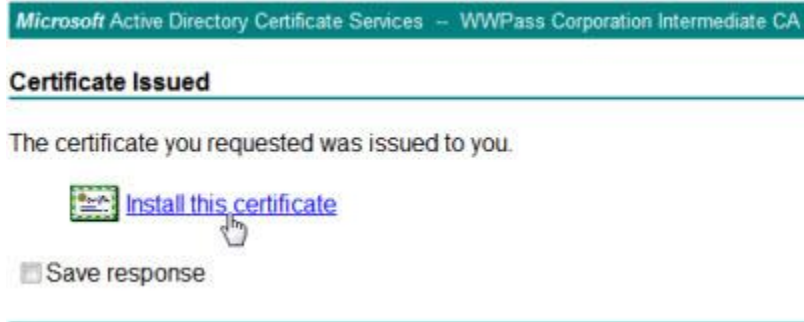
**View the Status of a Pending Certificate Request**

Select the certificate request you want to view:

[\(Thursday October 11 2012 12:47:04 PM\)](#)





- 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 it for authentication with Outlook and OWA.






## Import a Certificate Using the WWPass Dashboard

If your certificate is in a file, follow the steps below to import the certificate for use with your PassKey using the WWPass Dashboard.

### To import a certificate using Dashboard

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



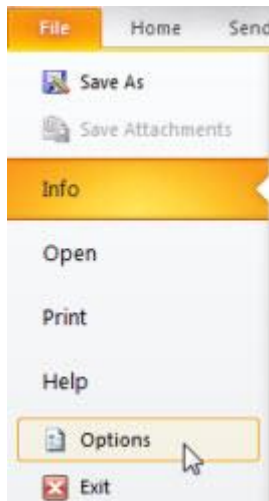
- From the Open Certificate window, locate the certificate file. Look for an extension of .pfx or .p12. Select the file and click .
- If prompted for the password used to encrypt the certificate file, enter the password and click .
- Enter the access code for your PassKey and click .

## Select Certificates for Outlook

Follow the steps below to check which email certificate is selected for digital signing and encryption in Outlook. The correct certificate might already be selected. You can select a different certificate, if needed.

### To check on or select an email certificate:

1. Click the File Tab in Outlook. Then click **Options**.



2. Click **Trust Center** on the right.

3. Click **Trust Center Settings...** under Microsoft Outlook Trust Center.

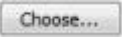
4. Click **E-mail Security**.

5. Select an email account from the list next to **Default Setting** on the E-mail Security tab and click **Settings...**. The Change Security Settings window opens. (If you only have one email account, the **Default Setting** list shows that account. If you have multiple accounts, the list shows the account selected last.)





**Note:** if you do not have Security Settings for an email account, you can add them by clicking **New** in the Change Security Settings window. Enter a name in the Security Settings Name box and click S/MIME in the Cryptography Format list. Depending on your certificate type, you can choose Exchange Security instead.



6. Verify that the correct certificate is shown next to **Encryption Certificate**. The certificate should be the one assigned by your company for use with Outlook. If that certificate is not shown, you can select it as follows:
  - a) Click .
  - b) Click the certificate in the **Select a Certificate** list.
  - c) Click **OK**.
7. Select the checkbox next to **Send these certificates with signed messages**. This ensures that your public key certificate is sent with all your digitally signed messages. People who receive your public key can send you encrypted messages and decrypt the messages you send them.
8. Click **OK** in the Change Security Settings window to save your settings.

## Install the S/MIME Control for OWA


Follow the steps below to install the S/MIME control for OWA. This control enables secure email functions.

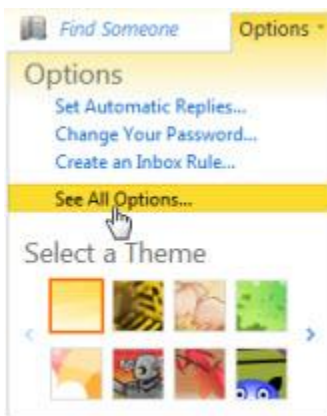
After the S/MIME control is installed, icons for digital signing  and encryption  are shown in the toolbar for new email messages.



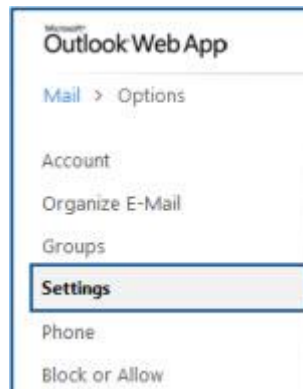
**Note:** If a message indicates you need to log in as an administrator in order to install the S/MIME control, ask a system administrator for assistance.

### To install the S/MIME control:

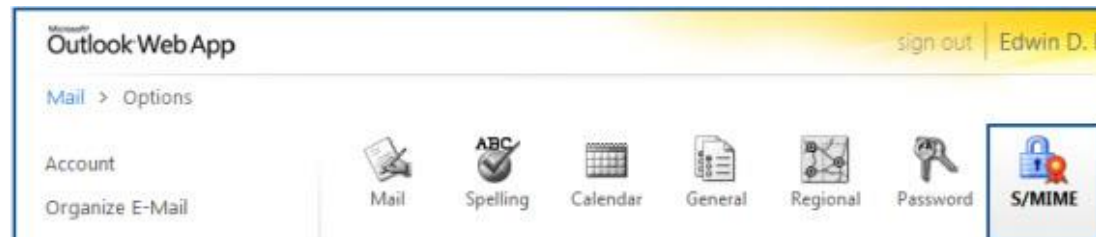
1. [Log into](#) OWA from Internet Explorer. The Outlook Web App page opens.
2. Click  on the right.
3. Click **See All Options** in the Options menu.



4. Click **Settings** on the left.




4. Click the **S/MIME** icon.



5. Click **Download the S/MIME control** under E-Mail Security.



6. When you are prompted to run or save the file, click . One or more verification prompts might appear. Click the **Run** button or option in each prompt. The S/MIME control is installed.

## Select Certificates for OWA

Follow the steps below to select the certificate to use for digital signing in OWA. You can select a certificate if:


- Your organization uses different certificates for logging into OWA and secure email.  
and
- The Select Certificate for Mail Signing feature is shown in OWA E-Mail Security options.

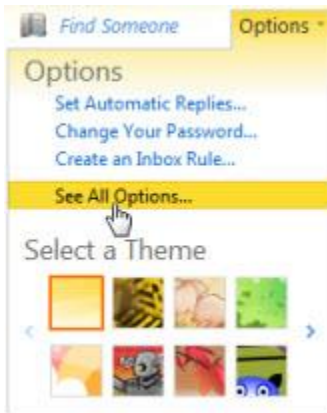
The email certificate you select is automatically for all digitally-signed messages you send.



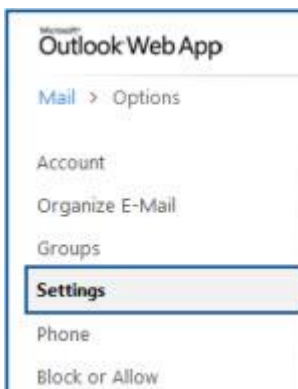
**Note:** Ideally, the certificate used for digital signing is one that is trusted outside your organization. If you do not select a widely-trusted certificate, the certificate you logged in with is used for digital signing. This certificate is trusted within your organization, but not outside it.

### To select a certificate for digital signing

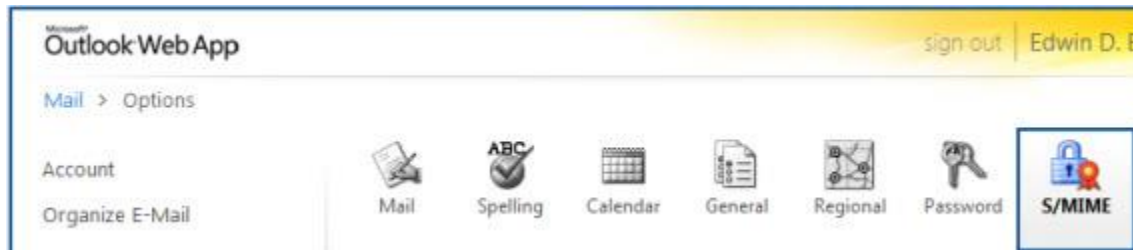
1. [Log into OWA](#) from Internet Explorer. The Outlook Web App page opens.
2. Click  on the right.
3. Click **See All Options** in the Options menu.



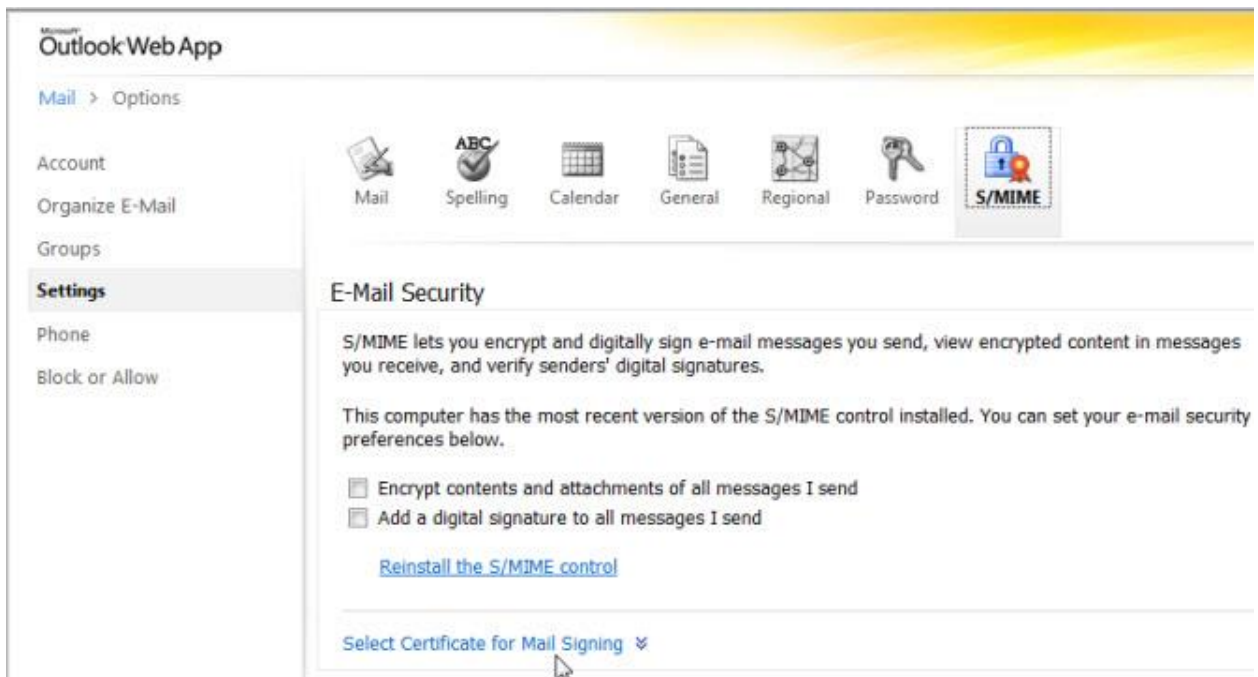
4. Click **Settings** on the left.



- Click the **S/MIME** button. The S/MIME tab appears.




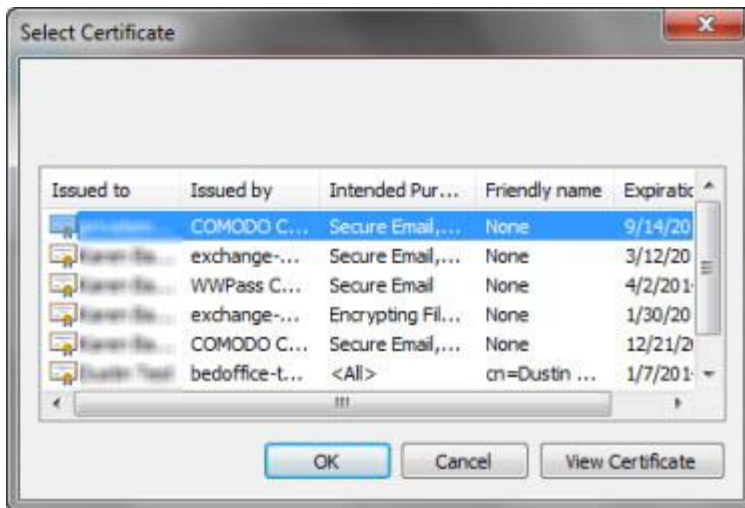
- Click **Select Certificate for Mail Signing** under E-Mail Security options.





- Select the **Manually choose the certificate** button. Then click Choose Signing Certificate.



8. From the Select Certificate window, look for the certificate designated by your organization as the one to use for digital signing. Select that certificate and click . (It can be the certificate used for Outlook.)



9. Click  in the lower right corner of the S/MIME tab to save your certificate selection.

 **Tip:** If you want to automatically encrypt and digitally sign all email messages, select checkboxes for **Encrypt contents** and **Add a digital signature** in the S/MIME tab. If you decide a certain message should not be encrypted or signed, you can unselect the encryption or digital signing option from the top of the message.

## E-Mail Security

S/MIME lets you encrypt and digitally sign e-mail messages you send, view encrypted content in messages you receive, and verify senders' digital signatures.

This computer has the most recent version of the S/MIME control installed. You can set your e-mail security preferences below.

- ☐ Encrypt contents and attachments of all messages I send
- ☒ Add a digital signature to all messages I send



## Share Public Keys for Exchanging Secure Email

Before you can exchange encrypted messages with someone, you need their public key (also known as a digital ID) and they need yours.

Your public key is part of your email certificate. You can share your public key with anyone. Only you have access to your private key.


Once you have someone's public key, you can encrypt the messages you send them.

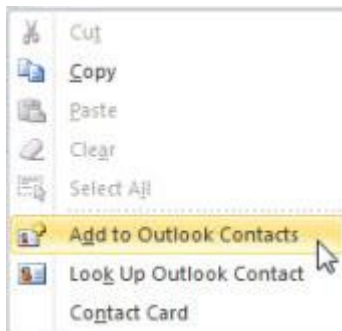
Follow the steps below to share public key certificates. The main steps are to exchange digitally signed emails and add correspondents to your Contacts lists.



**Note:** Coworker public keys are automatically available if your email system stores certificates centrally and associates them with Outlook accounts. This might be the case if your organization uses the Microsoft Exchange Server and a Global Address List. In this case, you can use a coworker's public key by selecting their name from the Global Address List.

### To share public keys

1. Ask an email correspondent to send you a digitally signed message.
2. Open the message from your Outlook Inbox. A digitally signed message is indicated by this icon .
3. Right-click the correspondent's name in the message.
4. Click **Add to Outlook Contacts**. The correspondent's public key certificate is stored with their contact information in your Contacts List.



5. Send the correspondent a digitally signed message and ask them to perform steps 2 thru 4. You and the correspondent can now exchange encrypted email messages.



## CHAPTER 5 — USING A PASSKEY WITH OUTLOOK

---

This chapter covers how to use a PassKey to authenticate your identity for secure email in Outlook.

### Topics In This Chapter

---

- [Overview](#)
- [Use a PassKey for Digital Signing in Outlook](#)
- [Use a PassKey for Encrypted Email in Outlook](#)

## Overview for Using a PassKey with Outlook

Once WWPass Security for Email (Outlook) is set up, you can use your PassKey in order to securely:


- [Send](#) digitally-signed emails from Outlook.
- [Decrypt](#) the encrypted emails you receive in Outlook.

Outlook checks for your PassKey when you try to send a digitally-signed email message or open an encrypted message:

- If your PassKey is not presented to your computer, you are prompted to present it (a message asks you to insert a smart card). You are then prompted for your PassKey access code.
- If your PassKey is presented to your computer, you are only prompted for your access code.

## Use a PassKey for Digital Signing in Outlook


Follow the steps below to send digitally-signed email from Outlook using your PassKey.

To identify digitally-signed messages in your Inbox, look for this icon:  The icon is also shown at the top of digitally-signed messages.


Click the icon in a signed message to view information on whether the digital signature is valid and trusted. To see more information about the digital signature, click **Details** in the information window.




To see the email address of the person who signed a message, check the **Signed By** line at the top of the message. (The **From** line shows who sent the message.)

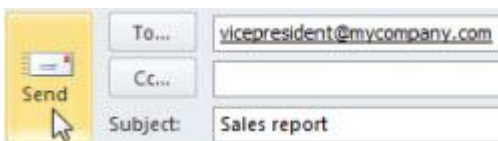
 **Tip:** To configure Outlook to digitally sign all messages, click Outlook File tab > Options > Trust Center > Trust Center Settings > E-mail Security. Then, Under Encrypted Mail in Email Security options, select the checkbox for **Add digital signature to outgoing messages**. Click **OK** to close each open Outlook screen.


## To send a digitally-signed message in Outlook

1. Present your PassKey to your computer by placing it on an NFC reader or inserting it into a USB port.
2. Create an email message in Outlook.
3. Click  Sign in the Options ribbon.




4. Click  Send to send the message.




5. If prompted for your WWPass access code, enter the access code for your PassKey and click  . The signed email message is sent.



 **Note:** A message asks you to insert a Smart Card if your PassKey is not present when you try to send a signed email. Place your PassKey on an NFC reader or insert it into a USB port, click **OK**, and enter your access code when prompted.

## Use a PassKey for Encrypted Email in Outlook

Follow the steps below to decrypt encrypted messages in Outlook using your PassKey. Attachments to the messages are also decrypted. A PassKey is not needed to send [encrypted messages](#).


To identify encrypted messages in your Inbox, look for this icon: 

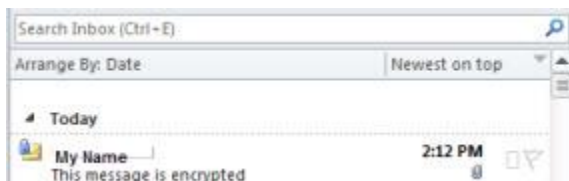
After you authenticate with your PassKey, a decrypted message can be viewed in the Outlook Reading Pane or by opening the message.


When you click an encrypted message in your Inbox before authenticating with your PassKey, the following is shown in the Reading Pane:

 This item cannot be displayed in the Reading Pane. Open the item to read its contents.


### To decrypt a message in Outlook

1. Present your PassKey to your computer by placing it on an NFC reader or inserting it into a USB port.
2. From your Outlook Inbox, click on an encrypted message. A lock icon  is shown beside it.





3. When prompted for your WWPass access code, enter the access code for your PassKey and click . The encrypted message is displayed in the Reading Pane. Double-click the message to open it.



 **Note:** A message asks you to insert a Smart Card if your PassKey is not present when you try to decrypt a message. Place your PassKey on an NFC reader or insert it into a USB port, click **OK**, and enter your access code when prompted.

## Basics for encrypted messages

- To encrypt a message, click the  **Encrypt** icon in Outlook's Options ribbon for a new message.
- If you want to automatically encrypt all messages, click File tab > Options > Trust Center > Trust Center Settings > E-mail Security. In Email Security options, select the checkbox for **Encrypt contents and attachments for outgoing messages**. You will not need to click the  **Encrypt** icon in Outlook's Options ribbon for each message you want to encrypt.



**Note:** Before you can send an encrypted message to someone, you need their public key. See [Sharing Public Keys](#).

## CHAPTER 6 — USING A PASSKEY WITH OWA

---

This chapter covers how to use a PassKey to authenticate your identity for secure email in OWA (Outlook Web App). It also covers how to use a PassKey to log into OWA and ECP (Exchange Control Panel), a tool for administrators.

### Topics In This Chapter

---

- [Overview](#)
- [Use a PassKey for Logging into OWA](#)
- [Use a PassKey for Logging into ECP](#)
- [Use a PassKey for Digital Signing in OWA](#)
- [Use a PassKey for Encrypted Email in OWA](#)





## Overview for Using a PassKey with OWA

Once WWPass Security for Email (Outlook) is set up for use with OWA, you can use your PassKey to securely:

- Log in to [OWA](#).
- Send digitally-signed emails from [OWA](#).
- Decrypt the encrypted emails you receive in [OWA](#).

After you present your PassKey to your computer and log into OWA, leave your PassKey in place so that you can use it for digital signing and decryption.

### Before you begin

- Before you can use secure email functions in OWA, the S/MIME control must be installed. Click [here](#) for the steps to follow. After the control is installed, icons for the digital signature  and encryption  functions are shown in the toolbar for new email messages.
- If your organization uses different certificates for OWA login OWA and secure email, [select](#) the certificate for secure email before you send digitally-signed email.

## Use a PassKey for Logging into OWA



Follow the steps below to log into OWA using your PassKey. Before you begin, ask a system administrator for the address (URL) for your OWA mailbox.

OWA checks for your PassKey when you log in:

- If your PassKey is not presented to your computer (via an NFC reader or USB port), you are prompted to present it (a message asks you to insert a Smart Card). You are then prompted for your PassKey access code.
- If your PassKey is in presented to your computer, you are only prompted for your access code.

### To log into OWA with a PassKey

---

1. Present your PassKey to your computer by placing it on an NFC reader or inserting it into a USB port.
2. Enter the address for your OWA mailbox in the Internet Explorer Web browser and press **Enter**.
3. If prompted to select a certificate, click on your OWA login certificate in the list that appears. Then click .
4. When prompted for your WWPass access code, enter the access code for your PassKey and click . The Outlook Web App page for your email account opens.

## Use a PassKey for Logging into ECP

If you are an administrator, follow the steps below to log in to ECP (Exchange Control Panel) using your PassKey. Your PassKey must be set up as described in the [Smart Start](#) for administrators.

### To log into ECP with a PassKey

---

1. Present your PassKey to your computer by placing it on an NFC reader or inserting it into a USB port.
2. Enter the URL for your ECP account in Internet Explorer and press **Enter**.
3. Respond to prompts as follows:
  - If prompted to select the certificate to use, click on the certificate in the list that appears. Then click **OK**.
  - When prompted for your WWPass access code, enter the access code for your PassKey and click **OK**. The page for your ECP account opens.

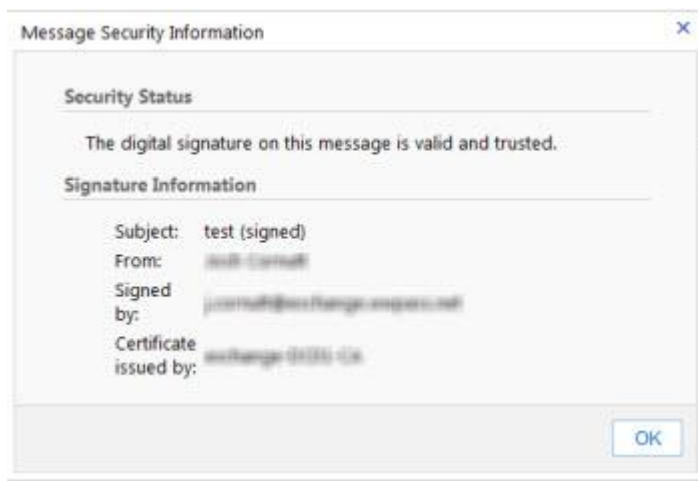


## Use a PassKey for Digital Signing in OWA

Follow the steps below to send digitally signed email from OWA using your PassKey.


To identify digitally-signed messages in your Inbox, look for this icon: 

Click the icon in a signed message to view information on whether a signature is valid and trusted.




**Tip:** To configure OWA to add your digital signature to all messages, go to the top of the Outlook Web App page and click Options > Settings > S/MIME tab. Then select **Add a digital signature to all messages I send**.

## To send a digitally-signed in OWA

1. With your PassKey presented to your computer (via an NFC reader or USB port), create an email message in OWA.
2. Click the "add a digital signature" icon  in the OWA toolbar for a new message. (Icon is shown when the [S/MIME control](#) is installed.)



3. Click **Send** in the OWA toolbar to send the message. Your PassKey is automatically used to authenticate you and the signed message is sent. (If prompted for your WWPass access code, enter the access code for your PassKey and click .)



**Note:** A message asks you to insert a Smart Card if your PassKey is not present when you try to send a signed message. Place your PassKey on an NFC reader or insert it into a USB port, click **OK**, and enter your access code when prompted.



## Use a PassKey for Encrypted Email in OWA

Follow the steps below to decrypt encrypted messages in OWA using your PassKey. Their attachments are also decrypted.


To identify the encrypted messages you receive, look for this icon: 

After you authenticate with your PassKey, a decrypted message can be viewed by opening the message. Text for decrypted messages is not shown in the OWA List View or Conversation mode.



### To decrypt a message in OWA

1. With your PassKey presented to your computer (via an NFC reader or USB port), go to your OWA Inbox and double-click an encrypted message. A lock icon  is shown beside it.
2. When prompted for your WWPass access code, enter the access code for your PassKey and click . The message is decrypted and opened. Any attachments are also decrypted.



 **Note:** A message asks you to insert a Smart Card if your PassKey is not present when you try to decrypt a message. Place your PassKey on an NFC reader or insert it into a USB port. Click **OK** in the next message and enter your access code when prompted.

### Basics for encrypted messages

- To encrypt a message, click the  icon in the OWA toolbar for a new message. (The icon is shown when the [S/MIME control](#) is installed.)
- If you want to automatically encrypt all messages, go to the top of the Outlook Web App page and click Options > Settings > S/MIME tab. Then select **Encrypt contents and attachments of all messages I send**. You will not need to click the  icon in the OWA toolbar for each message you want to encrypt.



**Tip:** Before you can send an encrypted message to someone, you need their public key. See [Sharing Public Keys](#).

