

Enabling Encrypted Email In Microsoft Outlook 2003/2007/2010

This help document provides step by step instructions for generating the public (.CER file) and private (.PFX file) keys necessary for you to receive encrypted e-mails. These are a matching pair of files like a lock and a key. It also provides instructions for how to copy these keys and install them.

Generate and Install Key

1. Using Internet Explorer, navigate to the following link:
<https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate>
2. Each time you are prompted with "This Web site is attempting to perform a digital certificate operation on your behalf:" Select "Yes"
3. Fill out form completely. Deselect "Opt In" for the newsletter (unless you wish to receive this newsletter). Select "I Accept" and click "Next"
4. After receiving the confirmation email, using Internet Explorer navigate to:
5. https://secure.comodo.net/products/!SecureEmailCertificate_Collec2
6. Enter the email address used in the first form. Enter the collection password specified in the confirmation email received above. (Repeat this step for each machine that you want to receive encrypted e-mails on for this e-mail address).

Backup Private Key (.PFX file)

1. While still in Internet Explorer, Select Tools->Internet Options
2. Then Content->Certificates
3. Highlight the certificate issued to your email address.
4. Click Export
5. Next
6. Select "Yes, export the private key", Next
7. Select "Personal Information Exchange - PKCS #12 (.PFX)"
8. Do not check any additional boxes, Next
9. Supply a password to secure your key, Next
10. Supply your email address as the filename (by default, this file will be saved on your desktop), Next
11. Finish
12. Copy the resulting file to a safe location that is backed up.

Create Copy of Public Key (.CER file)

1. While still in Internet Explorer,
2. Select Tools->Internet Options
3. Then, Content->Certificates
4. Highlight the certificate issued to your email address.
5. Click Export
6. Next

7. Select "No, do not export the private key", Next
8. Select "Base-64 encoded X.509 (.CER)", Next
9. Supply "public-" your email address as the filename (e.g. public-user@destwin.com)(by default, this file will be saved on your desktop. Store this file in a safe location.
10. Compose an email message to support@destwin.com.
11. Attach your public certificate (.CER file) to that email.
12. If you are prompted with "This item contains attachments that are potentially unsafe." Select "Yes" to send anyway.

Completing the above will result in support@destwin.com receiving an e-mail from you with a .CER file attached. We will install this .CER file on our server and you will be able to receive encrypted e-mails from us on the computer that you installed your .PFX file on.

The instructions below pertain to installing your .PFX file on an alternate or additional computer so that you can receive encrypted e-mails from us on that computer.

Install Private Key (.PFX file) on a New or Alternate Computer

1. On the old computer open Internet Explorer, Select Tools->Internet Options
2. Then Content->Certificates
3. Highlight the certificate issued to your email address.
4. Click Export
5. Next
6. Select "Yes, export the private key", Next
7. Select "Personal Information Exchange - PKCS #12 (.PFX)"
8. Do not check any addition boxes, Next
9. Supply a password to secure your key, Next
10. Supply your email address as the file name (by default, this file will be saved to your Documents folder), Next
11. Finish
12. Copy the resulting file to the new computer.
13. On the new computer open Internet Explorer, Select Tools->Internet Options
14. Then Content->Certificates
15. Click Import
16. Next
17. Click browse and locate the exported file (you may have to select Personal Information Exchange as the file type to see the file)
18. Next
19. Enter the password from step 9.
20. Check "Mark this key as exportable" and leave "Include all extended properties" checked, Next.
21. Next again and Finish.