

# Secure2email, Version 6: Product Tour

A quick visual guide to the features of secure2email

Avoco Secure

 [info@avocosecure.com](mailto:info@avocosecure.com)

US: +1 415 839 9433

International: +44 207 851 6070

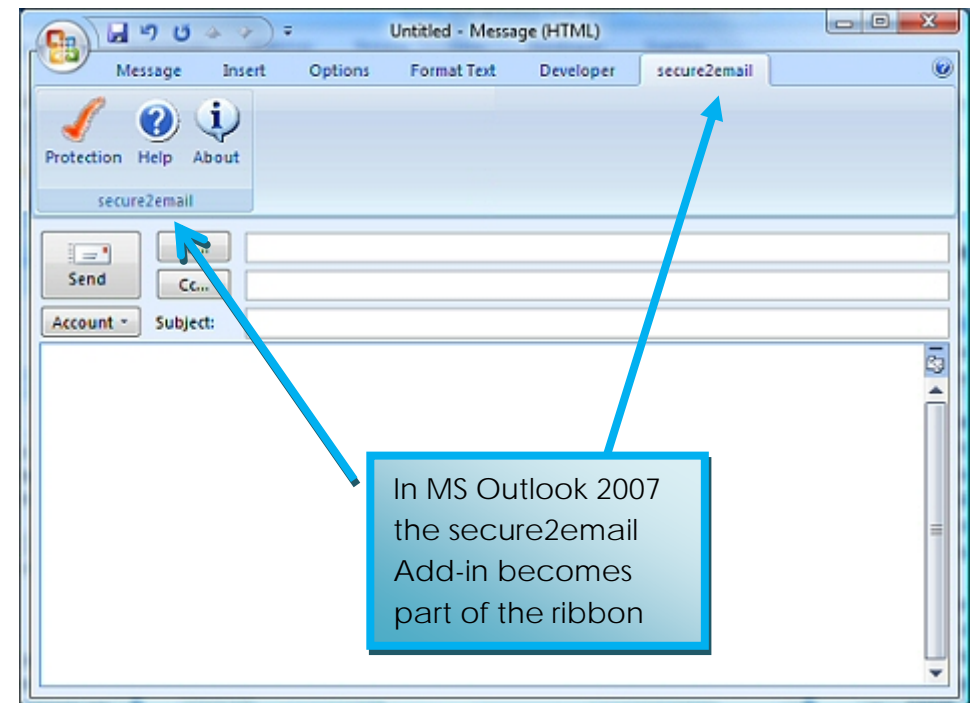
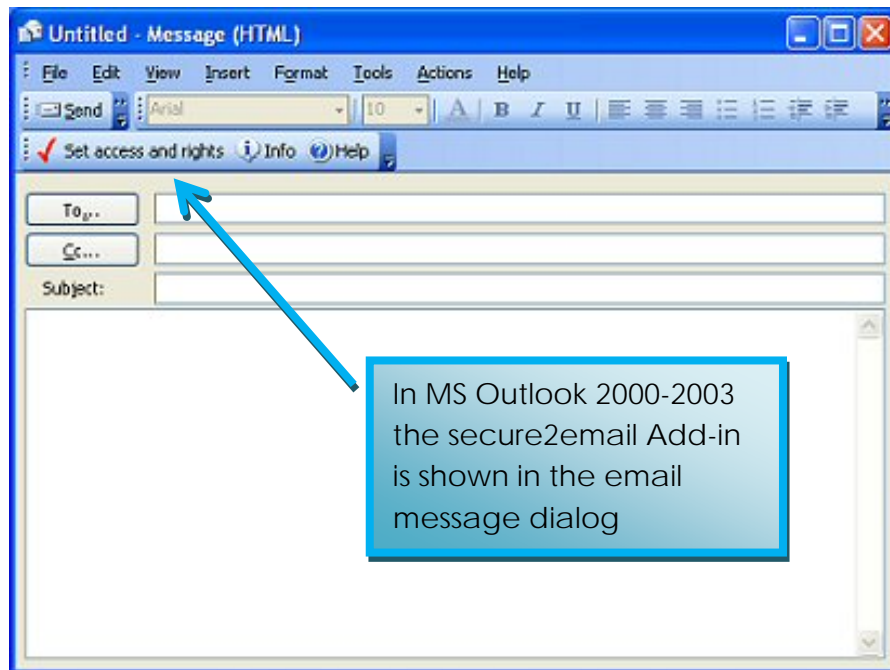
[www.avocosecure.com](http://www.avocosecure.com)

© Avoco Secure 2006 - All rights reserved.



# Direct Integration into Microsoft Outlook

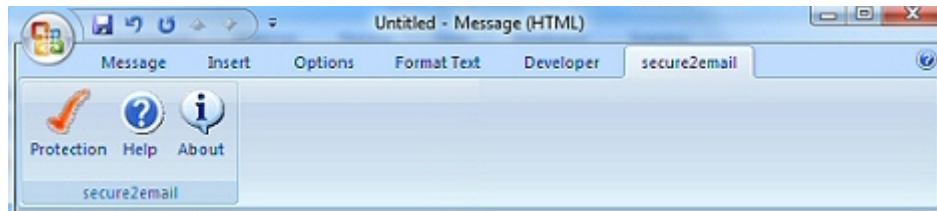
Secure2email installs in seconds and becomes an add-in into Microsoft Outlook 2000-2007



# Simple, Just Click to Protect Your Emails

Protect your emails: Set who can access the email and what can be done with the email after access

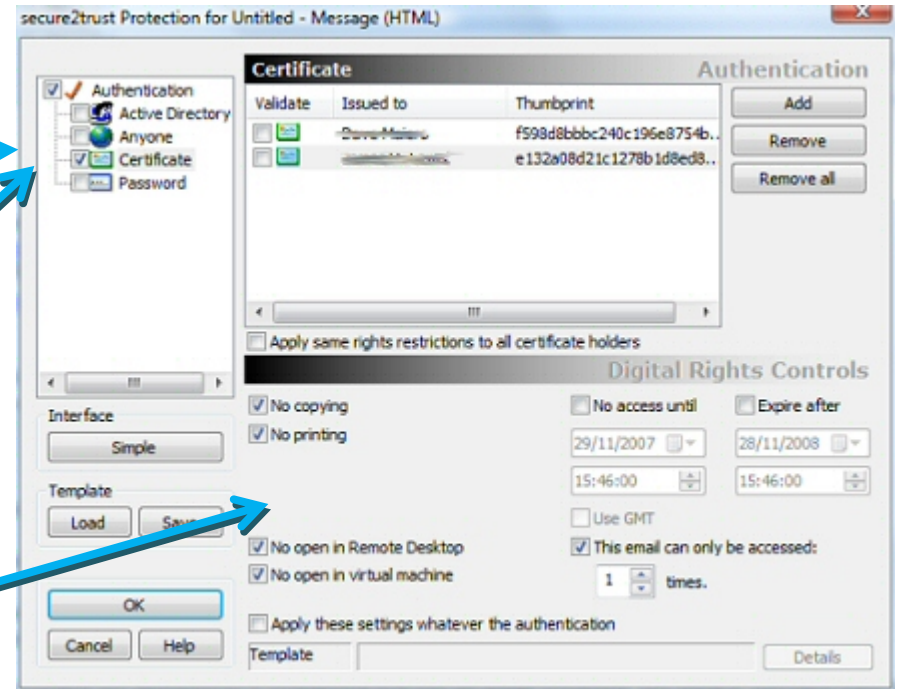
The secure2email dialog offers you protection options



Click Protection (2007) or set access and rights (2000-2003) to protect your email

Choose who can access your email

And what they can do with the email after access has been allowed



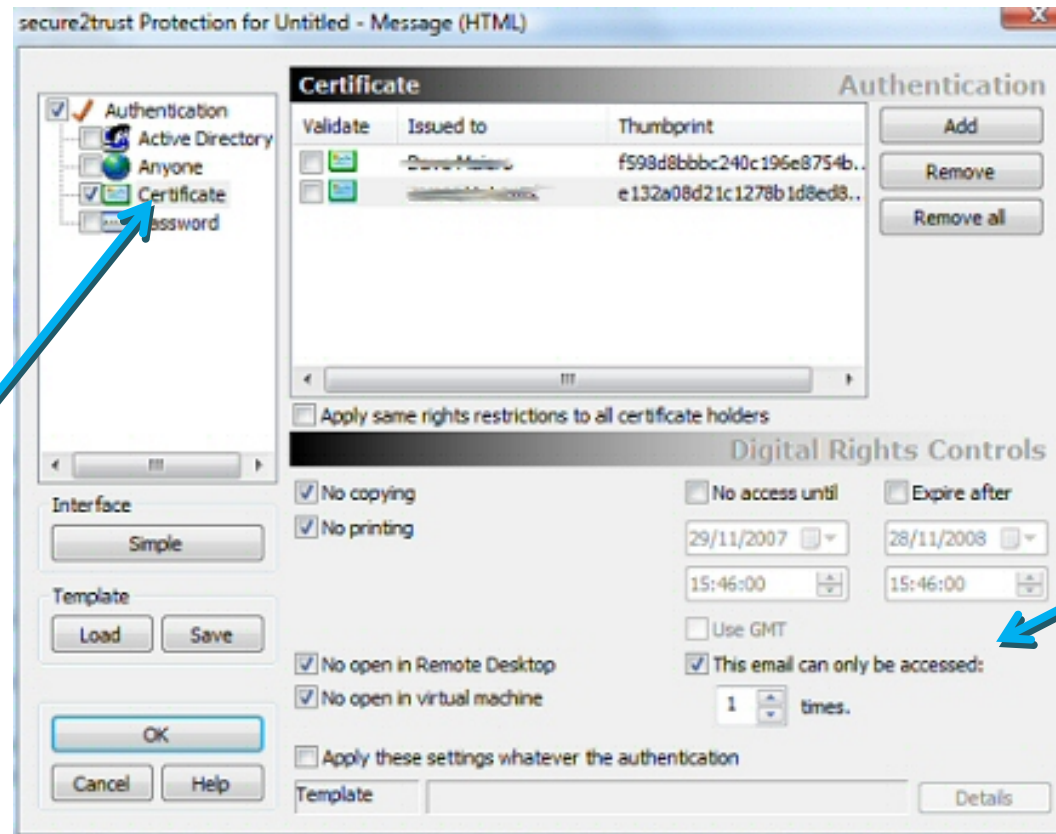
# Set who can access your email: Digital Certificate holder

Use an individual's identity, such as Active Directory membership or Digital Certificate ownership, or set a password, to access an email

Digital certificates are used to identify an individual. They are issued by a certificate authority (CA) who checks out the individual's identity, and then when they are satisfied that they are who they say they are, the CA will issue a certificate in that person's name.

To choose which digital certificate holders can access your email you will need the public key of the individual's digital certificate.

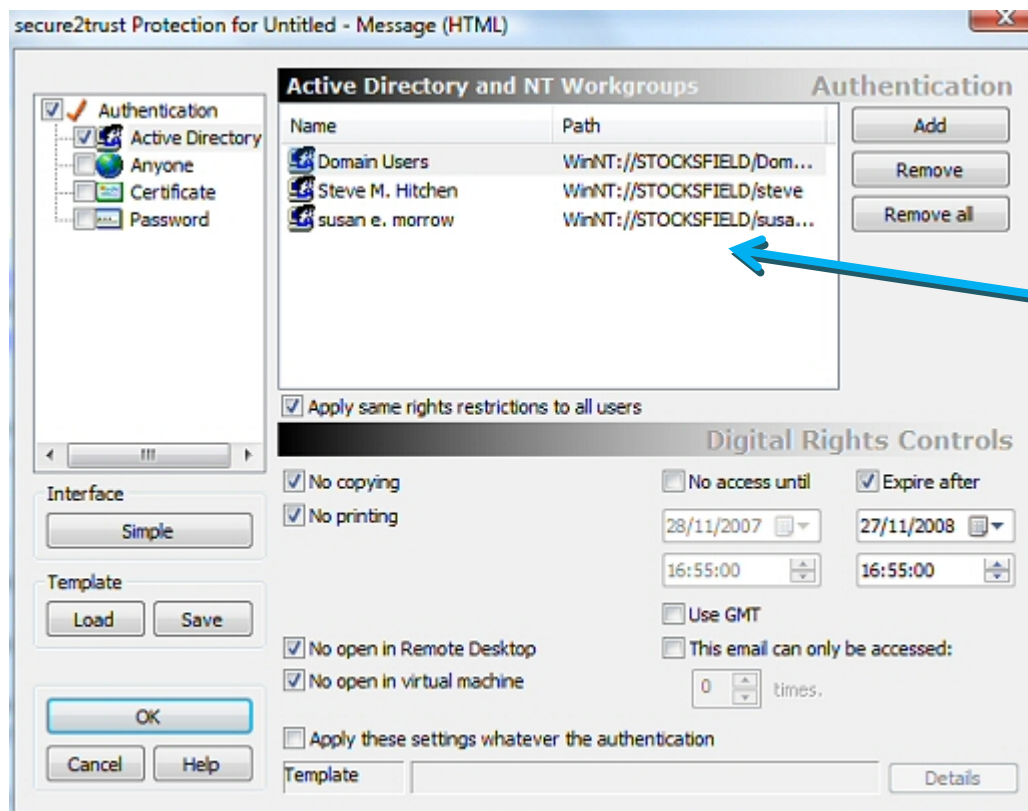
You can then check the 'Certificate' box under authentication in the secure2email dialog and click Add to choose the users who can access your email.



You can then choose restrictions on the use of your email for each user that can access your email (see below for more details on restrictions)

# Set who can access your email: Active Directory

Using Active directory to control who can access an email is a useful method of ensuring that emails do not go outside of your company network



To ensure that only certain members of your company network can access an email, choose these individuals (or groups) from your active directory console.

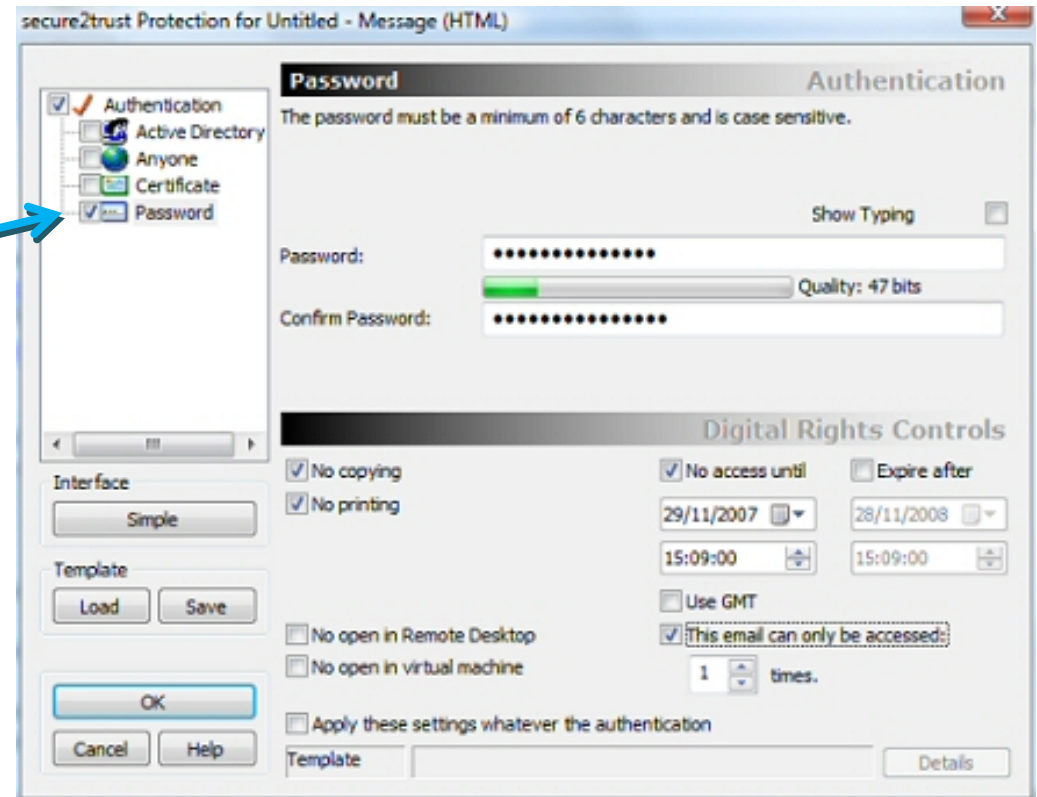
Check the Active Directory check box under authentication then click Add to open the Microsoft Active Directory console to choose who can access your email.

You can then associate restrictions on the use of the email with each chosen user

# Set who can access your email: Password

A password can also be set to access an email; a recipient will be requested to enter the correct password before access to the email is allowed.

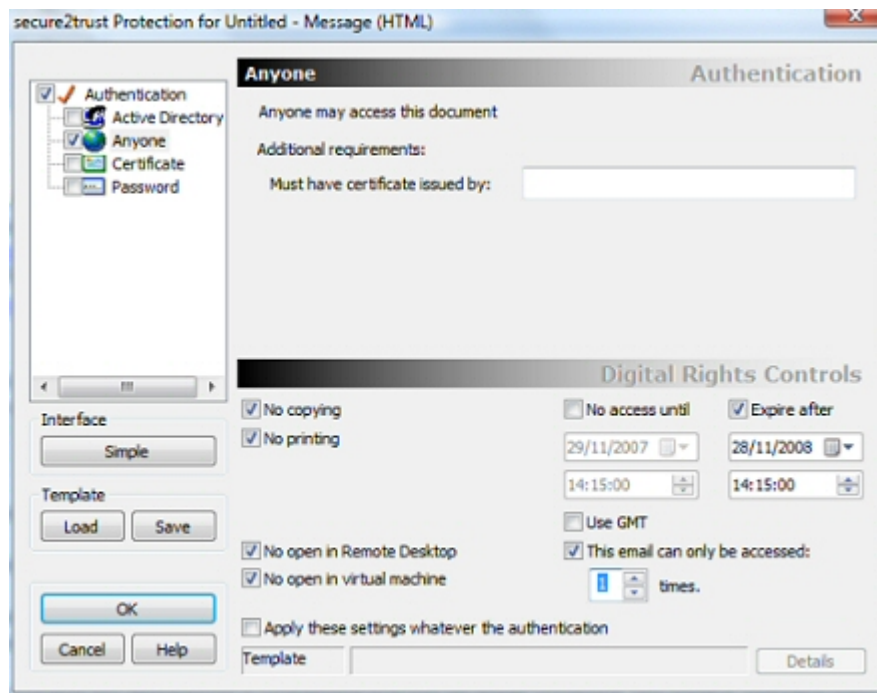
Restrictions on the use of the email are applied to all recipients entering the correct password.



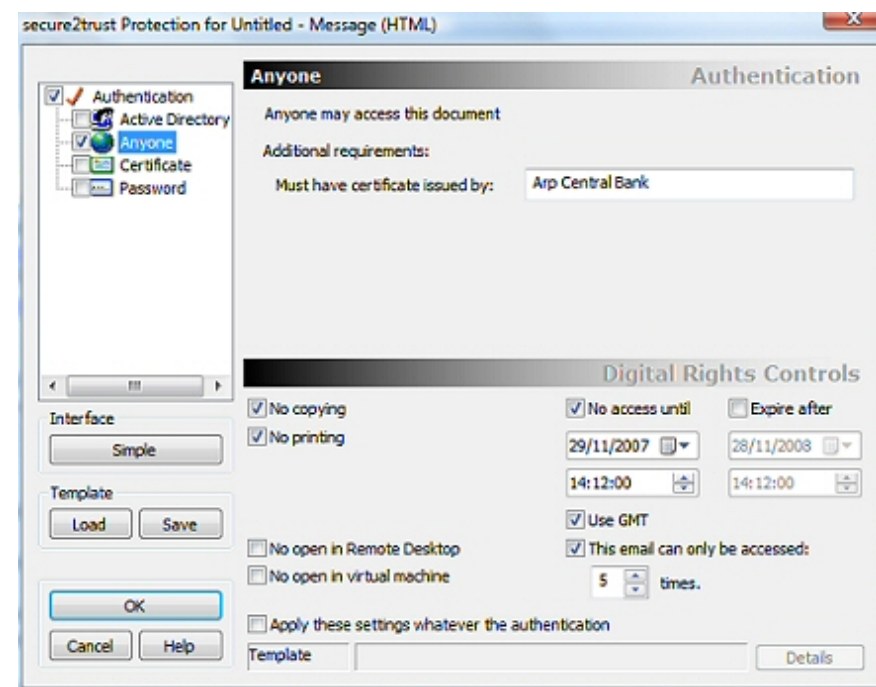
# Set who can access your email: Anyone

You can set access to an email so that no identifier is required, i.e. anyone can access the email but the use of the email will be restricted.

In addition, you can extend the security of anyone access so that anyone can access the email if they also have a digital certificate issued by a specified certificate authority.



Check Anyone so that the email recipient does not need to prove their identity to access the email

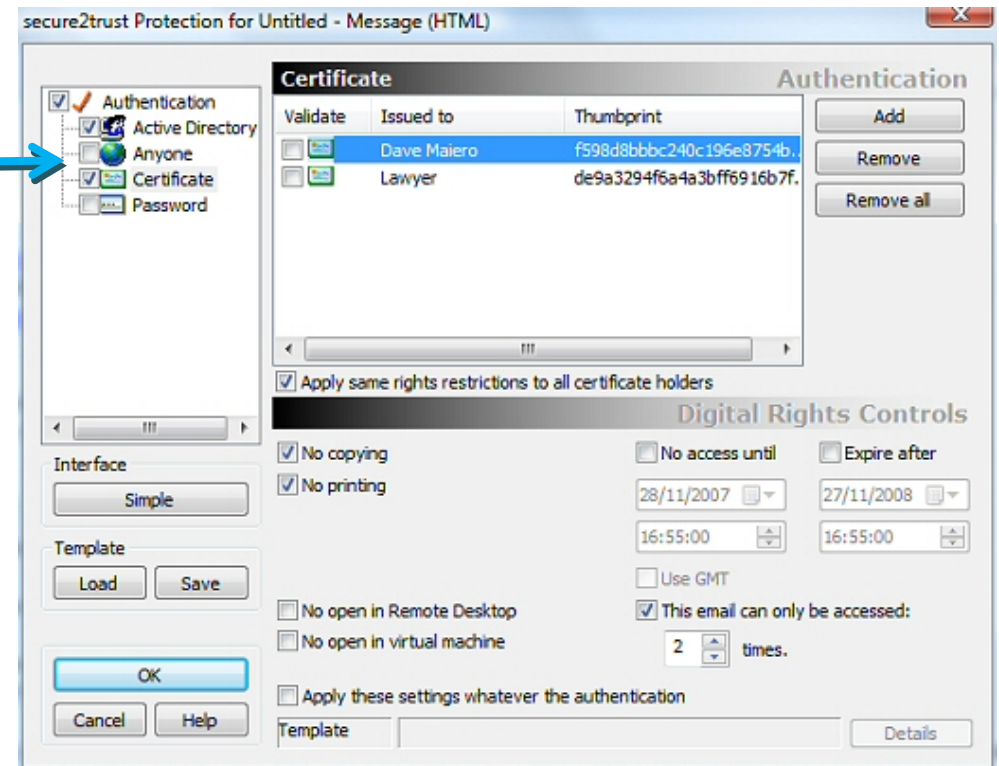


For additional security allow anyone access only if they also have a certificate issued by a specified certificate authority

# Set who can access your email: Using multiple methods of identity

If an email is especially sensitive you can set access to be only allowed if the recipient can prove twice or even three times that they are that correct person.

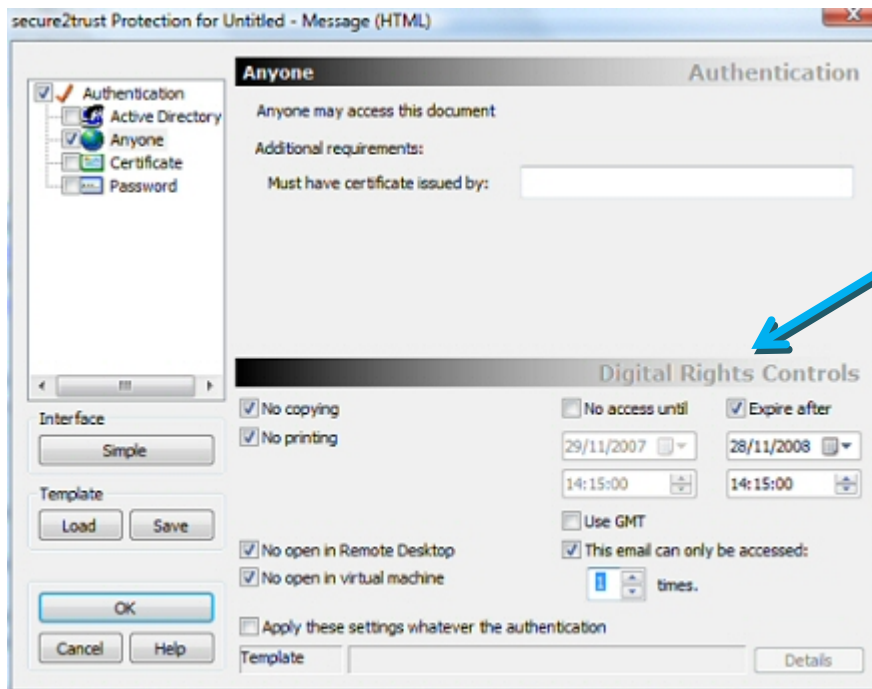
For example you can set access to be only allowed if the user has the correct active directory logon and has a digital certificate issued in their name. In addition, you could also specify that they need to enter a password too before access is granted.



Alternatively, you can set the email so that more than one user can access it but each user needs a separate method of identifying themselves and the restrictions on the use of the email are different for each recipient. For example, if you are a specified active directory member then you can access the email 25 times but if you only have a password you can only access the email once.

# Decide how an email can be used

The rights restrictions that secure2email allow you to apply let you decide what a recipient can do with the email once they have accessed the email



Rights to the use of the email after access include:

No copying – the content of the email cannot be copied. This includes using third party screen capture programs

No printing – prevents the recipient printing the content of the email

No open in remote desktop – prevents the recipient accessing the email remotely and using it from that remote location

No open in virtual machine – prevents the use of virtualisation technology to access the email

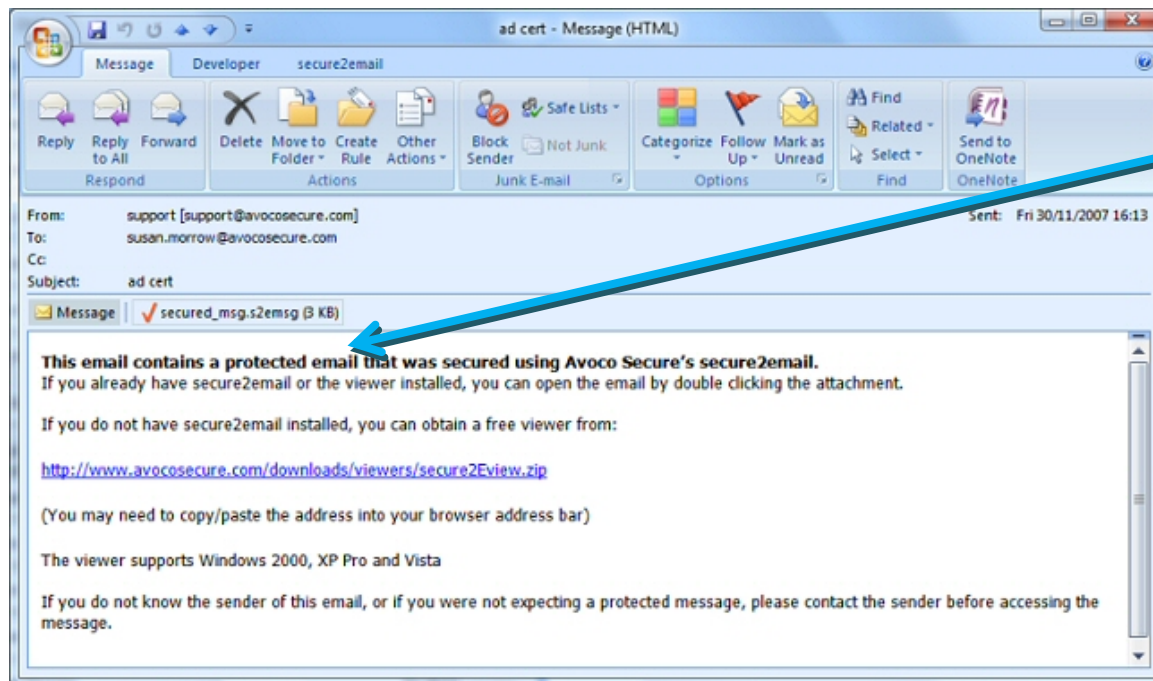
Time restrictions on the day and time that the email may be accessed

The number of times the email can be accessed

# Sending your protected email

Just click OK to set your protection then click Send as normal

Protected emails can be accessed using any email client both on the desktop and online (e.g. hotmail, Gmail, etc.)



Recipients receive an email similar to this email in their email client as normal.

The protected email is carried to the recipient in this email.

To access the protected email the recipient will need to have either the full secure2email program installed or a free viewer.

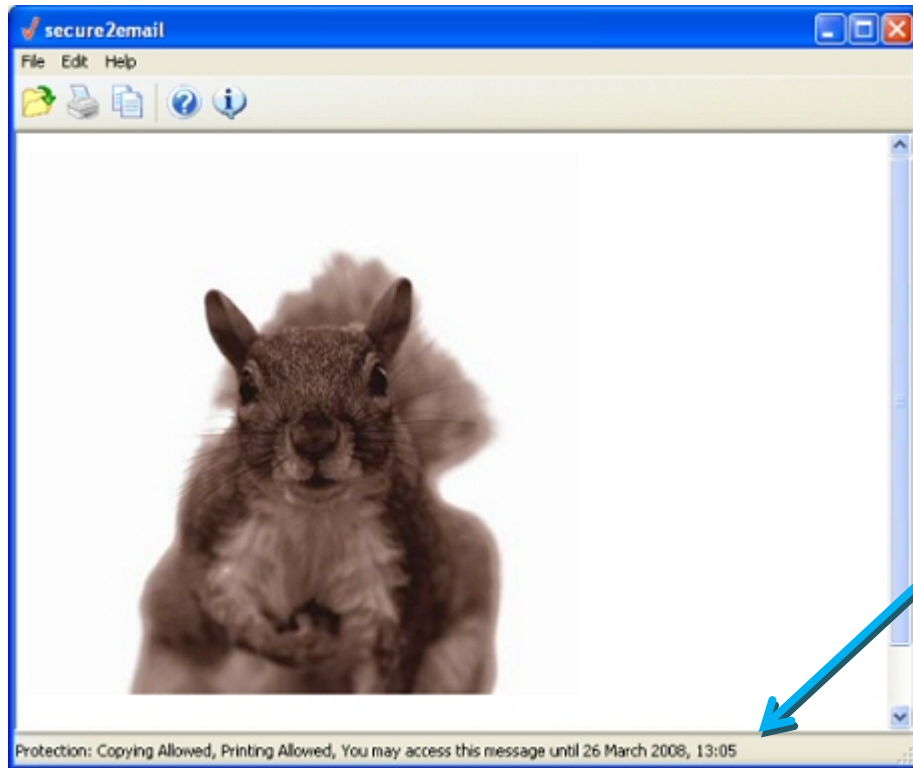
They then simply double click on the attachment and if they are the correct person set to access the email it will open.

A free viewer for recipients of protected emails can be downloaded here (2MB):

<http://www.avocosecure.com/downloads/viewers/secure2Eview.zip>

# Accessing the protected email

Protected emails can be accessed in any email client as long as the recipient has the secure2email full program or viewer installed.



On successfully accessing the email the message will open in the viewer. Using a viewer ensures that any email client that the recipient uses is supported.

The protection settings applied to the message are shown in the status bar at the bottom of the message.