How To Use MDaemon's PGP

With the release of MDaemon v15.5.0 users now have a built-in method to use PGP. Having OpenPGP built in to MDaemon simplifies the process of PGP key management, and encrypting/decrypting emails. MDPGP is free to use for all MDaemon sites running MDaemon v15.5.0 or higher.

How does PGP work?

Each account using PGP has 2 "keys" that belong to them. A *private key* and a *public key*. These keys are used to encrypt/decrypt emails sent to you. As the name of these keys suggest one key is meant to be kept private, and the other key is meant to be made public.

Below are examples of when these keys will be used.

Someone sends you an email: In order for the email to be encrypted by the sender, and decrypted by you, the sender encrypts the message using *your* public key. The email is then decrypted using your *private* key.

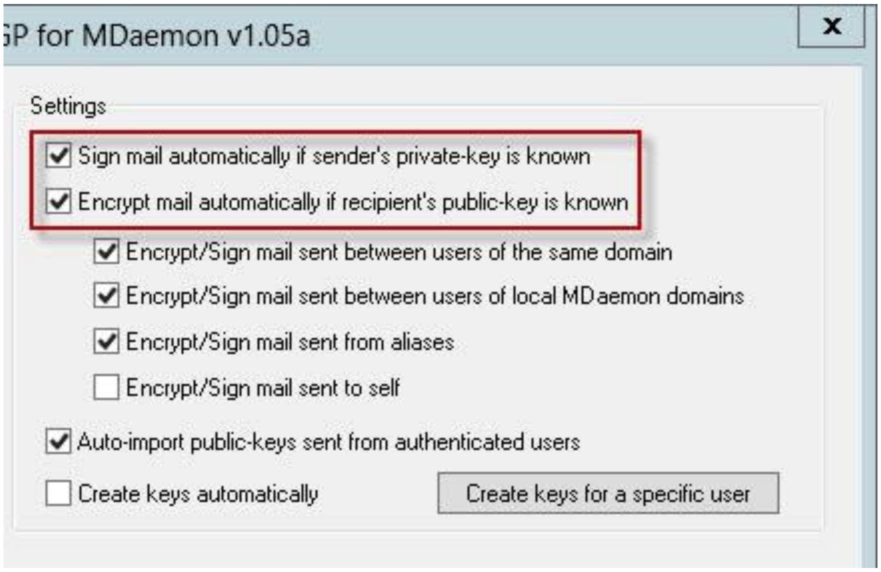
You send someone an email: In order for the email to be encrypted you are going to send you'll need to use the recipient's *public* key. The recipient will then decrypt the message using their own private key.

More in depth information can be found here.

MDaemon's PGP implementation has two modes of operation.

1. **Automatic Mode:** MDaemon will automatically encrypt emails if the recipient's public key is known. Meaning the recipient's public key is found in MDaemon's list of known public keys. No user intervention is required to encrypt emails.

   This is the default option for MDaemon PGP. MDaemon's PGP settings can be found by clicking Security | MDPGP.



GP for MDaemon v1.05a

Settings

☑ Sign mail automatically if sender's private-key is known

☑ Encrypt mail automatically if recipient's public-key is known

☑ Encrypt/Sign mail sent between users of the same domain

☑ Encrypt/Sign mail sent between users of local MDaemon domains

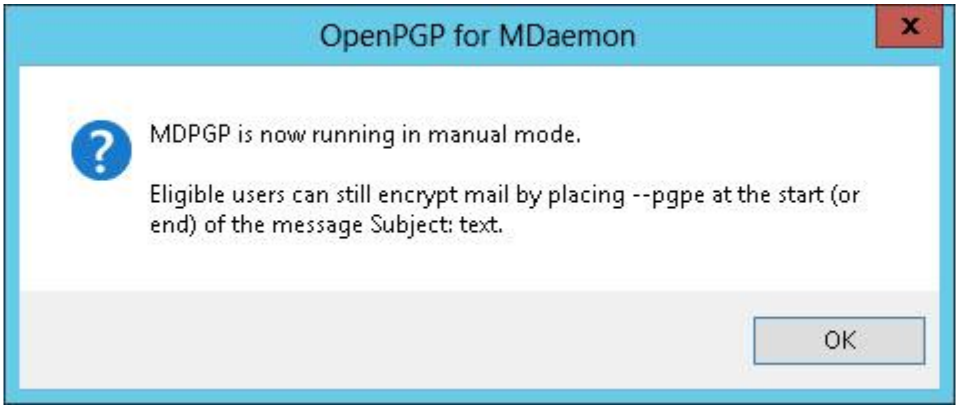
☑ Encrypt/Sign mail sent from aliases

□ Encrypt/Sign mail sent to self

☑ Auto-import public-keys sent from authenticated users

□ Create keys automatically

2. **Manual Mode:** To enter in to Manual Mode simply remove the check mark from either option shown in the above screenshot boxed in red. MDaemon provides a warning when each option is deselected as shown below.



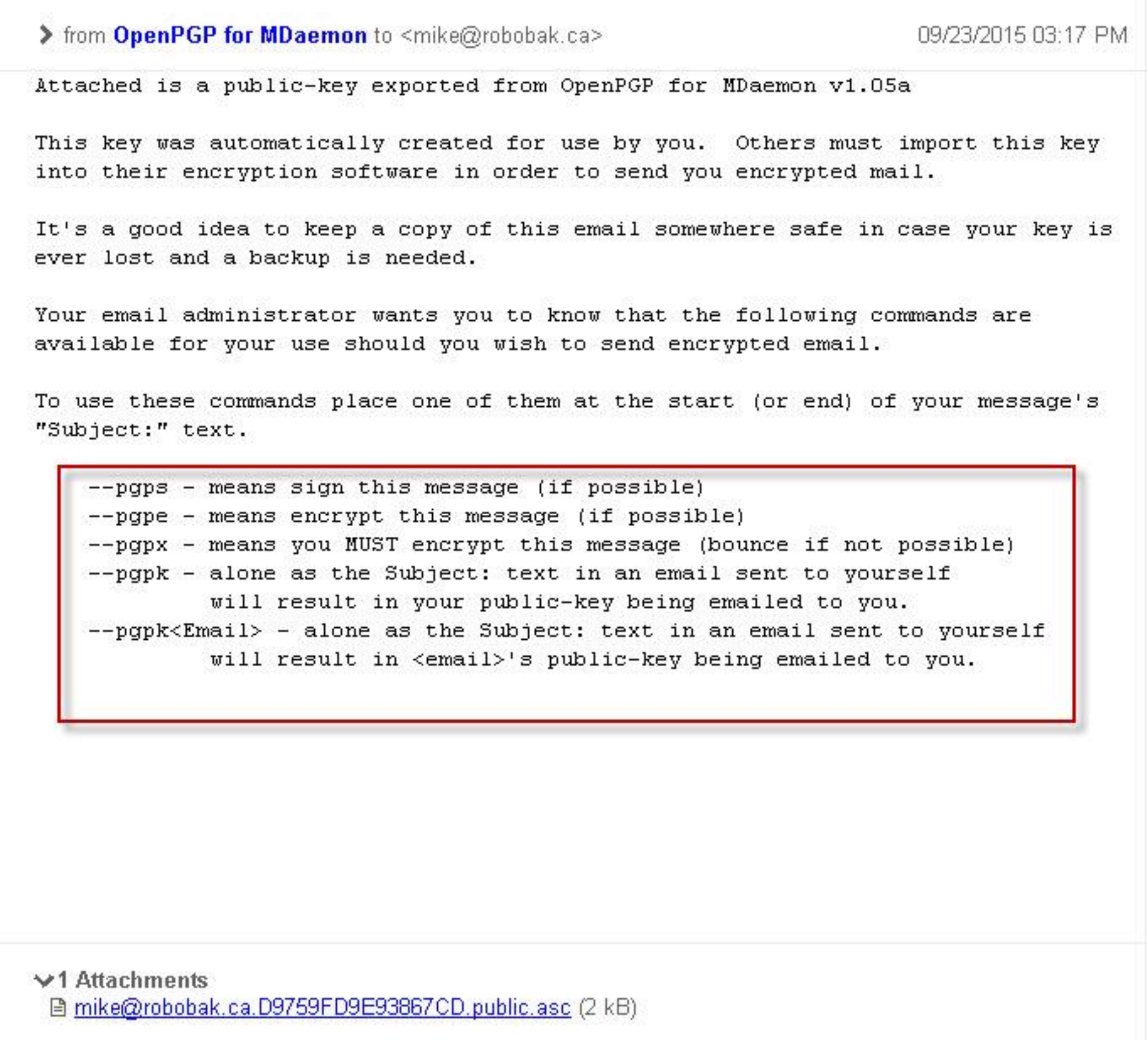
OpenPGP for MDaemon

MDPGP is now running in manual mode.

Eligible users can still encrypt mail by placing --pgpe at the start (or end) of the message Subject: text.

With Manual Mode users will need to choose which messages are encrypted. If the user chooses not to encrypt then the email they send is delivered in standard format (no encryption). To encrypt a message the user must prepend, or append, the appropriate command that tells MDaemon to encrypt the email.

When you create keys for a user there is an optional setting to email the user their public key. This is so the user can distribute their public key to other users that they wish to receive encrypted emails from. When MDaemon sends the user's public key via email there are also instructions in the email as to what commands to use. An example of this is shown below.



from **OpenPGP for MDaemon** to <mike@robobak.ca> 09/23/2015 03:17 PM

```
Attached is a public-key exported from OpenPGP for MDaemon v1.05a

This key was automatically created for use by you.  Others must import this key
into their encryption software in order to send you encrypted mail.

It's a good idea to keep a copy of this email somewhere safe in case your key is
ever lost and a backup is needed.

Your email administrator wants you to know that the following commands are
available for your use should you wish to send encrypted email.

To use these commands place one of them at the start (or end) of your message's
"Subject:" text.

  --pgps - means sign this message (if possible)
  --pgpe - means encrypt this message (if possible)
  --pgpx - means you MUST encrypt this message (bounce if not possible)
  --pgpk - alone as the Subject: text in an email sent to yourself
           will result in your public-key being emailed to you.
  --pgpk<Email> - alone as the Subject: text in an email sent to yourself
           will result in <email>'s public-key being emailed to you.
```

1 Attachments

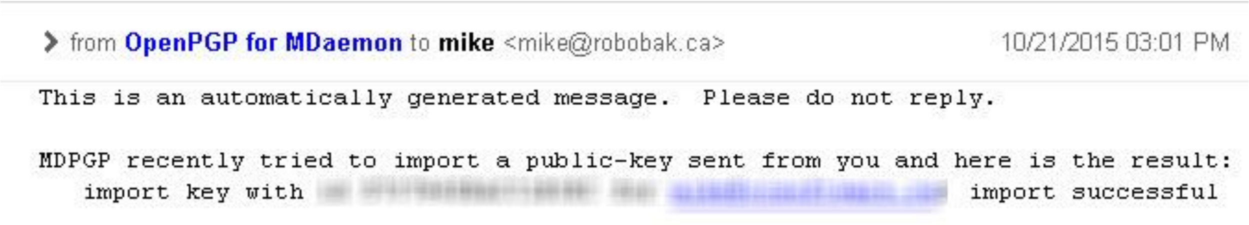
mike@robobak.ca.D9759FD9E93867CD.public.asc (2 kB)

I have received an email that has a user's public key attached. What do I do now?

Before you can send an encrypted email to this user the public key must first be imported on to your key ring. MDaemon makes this a very easy process Simply send a message to yourself with the public key attached. MDaemon will automatically detect the presence of the PGP public key and then imports it to the user's key ring. The user can now send encrypted messages to the user from whom they received the public key from.

*****NOTE:** MDaemon will only import the public key in an automatic fashion if the SMTP session used to send the email, with the public key attached, used *SMTP Authentication*.

MDaemon will report back to the user in the form of an email letting them know whether the import was successful, or if it failed. An example of a successful import is shown below.



> from **OpenPGP for MDaemon** to **mike** <mike@robobak.ca> 10/21/2015 03:01 PM

```
This is an automatically generated message.  Please do not reply.

MDPGP recently tried to import a public-key sent from you and here is the result:
   import key with [redacted] import successful
```

Once the public keys have been exchanged between two users, and imported, encrypted emails can then be sent between the two users.