

## PrivateFile Mail Gateway and ClearSwift MIMESweeper™ for SMTP 5™

### Tutorial – Person to Person

PrivateFile Mail Gateway integrates with **MIMESweeper for SMTP 5™** to encrypt sensitive emails and attachments as they are sent across the Internet. Unless secured, emails travelling across the Internet can be read by anyone who has access to the intermediate computers and servers.

#### Tutorial Overview

Using **PrivateFile Mail Gateway** and **MIMESweeper for SMTP 5™** you want to encrypt all email attachments going between one person in your company (**joe@YourCompany.com**) and one person in a partner company (**john@PrivateFile.Demo**). This tutorial shows the steps involved in setting this up. This tutorial uses the PrivateFile AES engine to encrypt the attachments. Most of the steps are setup using **MIMESweeper for SMTP 5™** while some use the **PrivateFile Mail Gateway** administration function

You will need to choose appropriate email addresses for your company and change the settings as you go down through this tutorial.

#### Prerequisites

The tutorial assumes that MIMESweeper for SMTP 5™ and PrivateFile Mail Gateway have already been installed on an appropriate server.

#### PrivateFile Mail Gateway Evaluation version

You can download an evaluation version of **PrivateFile Mail Gateway** from [www.private-file.com](http://www.private-file.com). This is a 30 day evaluation. This version permits the encryption of emails and attachments using the PrivateFile AES encryption engine.



#### PrivateFile Limited

Information Security Centre  
2052 Citywest Business Campus  
Co. Dublin  
Ireland

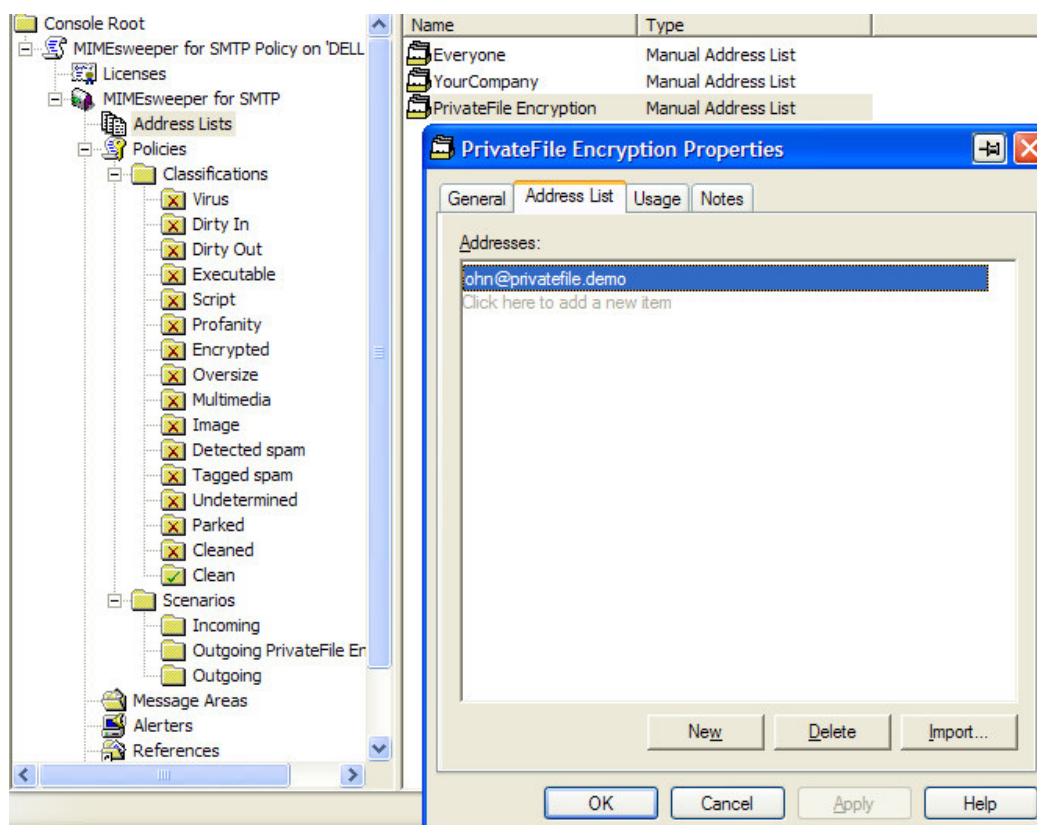
T +353 (0)1 642 0550  
F +353 (0)1 466 0468  
E [info@private-file.com](mailto:info@private-file.com)  
W [www.private-file.com](http://www.private-file.com)

## MIMESweeper for SMTP 5™ Steps

These steps are performed in the **MimeSweeper for SMTP Policy Editor**

### Address List

Create a new Address List called **PrivateFile Encryption**. This contains the filter [john@PrivateFile.Demo](mailto:john@PrivateFile.Demo).



This will be used to ensure that only emails being sent to **john** at domain **PrivateFile.Demo** will be sent through the **PrivateFile Encryption Scenario**

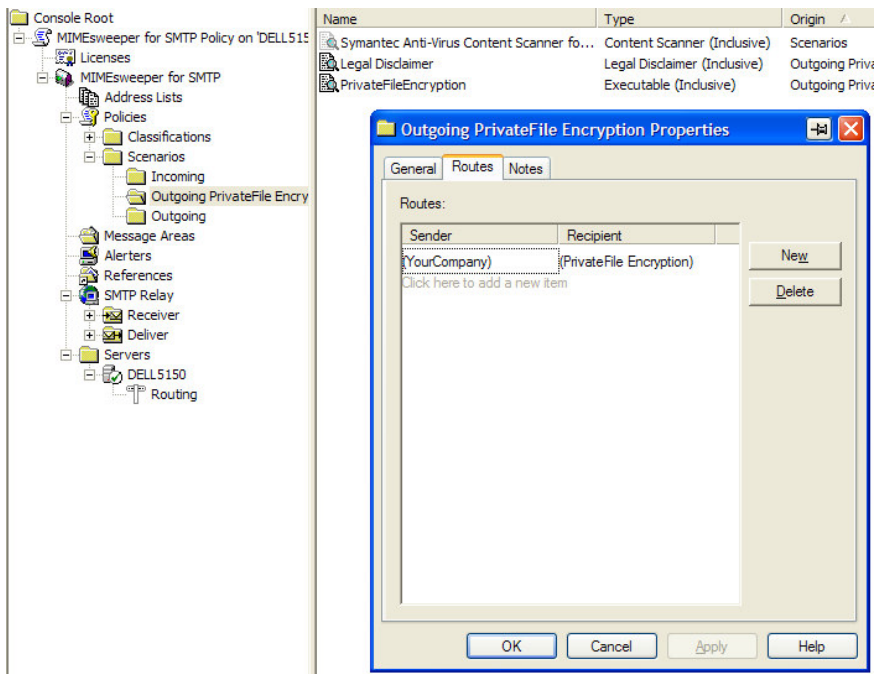
## Create Outgoing PrivateFile Encryption Scenario

This should be before the existing Outgoing Scenario. The routing should be set so that the

recipient is set to the **PrivateFile Encryption** mailing list which was setup in the previous step. This is to ensure that the necessary emails will be processed by the **PrivateFile Mail Gateway**.

In this scenario you can put the standard **Legal Disclaimer** etc.

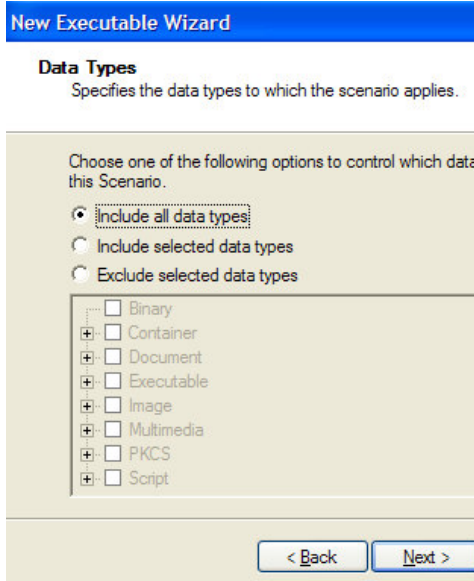
The last item in the scenario will be the call to the **PrivateFileEncryption Executable**.



## Create PrivateFileEncryption Executable

This step sets up the call to the **PrivateFile Mail Gateway** to encrypt the attachments.

In the **PrivateFile Encryption** scenario right-click and select **New** and then **Executable**. Click **Next twice** to go to the **Data Types** dialog. Choose **Include all data Types**



Click **Next** to go to the **Application Details Screen**

In the **Application filename** field enter **PrivateFile Mail Gateway**

In the **Command line** field enter **/O,%FILENAME%**

**/O** indicates to the **PrivateFile Mail Gateway** that this is an outbound email and so should be encrypted

**%FILENAME%** is the name of the message filename containing the email with the attachment to be encrypted

**New Executable Wizard**

**Application Details**  
Specify the application filename and the command line to be used. Use the token button to add tokens that will be replaced when the Scenario is executed.

Application filename: PrivateFileMailGateway

Application Type:  Win32  DOS

Command line: /O,%FILENAME% Token

Advanced  
The advanced dialog allows the timeout, file extension and mutex name to be configured. Advanced...

*By default, MIMESweeper expects to find the specified application on the system path of each of your configured servers.*

< Back Next > Cancel Help

Click **Next** for the **Return Codes** tab

Setup 2 Return Codes

For the first return code enter **0** and **NONE**

The **Mail Gateway** returns 0 if the email is not modified (e.g. there is no attachment)

The second return code should be set to **1** and **MODIFIED**. The **Mail Gateway** returns 1 if the email has been modified

**New Executable Wizard**

**Return Codes**  
Specifies how the return codes of the application should be interpreted. For each MODIFIED and DETECTED status, you can optionally add a description.

For each return code, enter the status that should be mapped to that code. You must enter at least one return code for either the DETECTED or MODIFIED status and at least one for the NONE status.

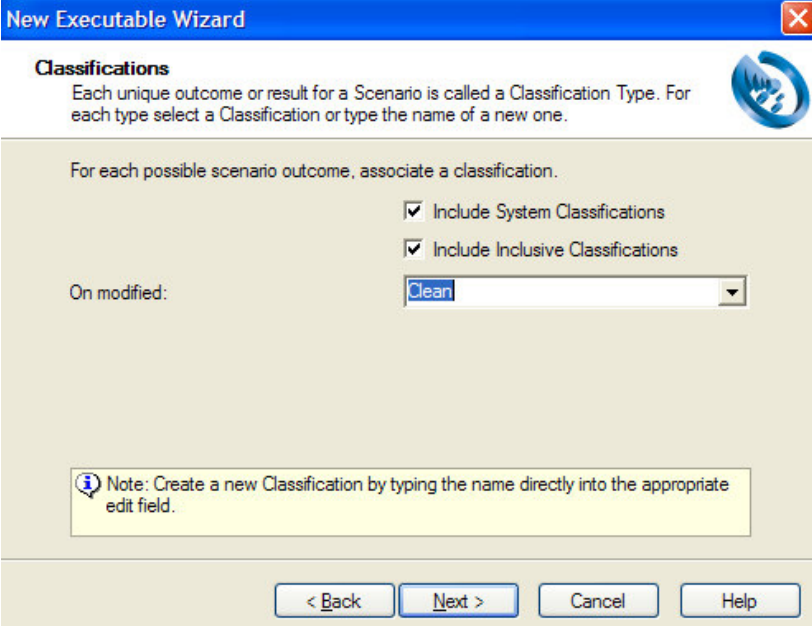
Return Code	Status	Description
0	NONE	
1	MODIFIED	
Click here to add a new item		

New Delete

< Back Next > Cancel Help

Click **Next** for the **Classifications** tab

Check both **Classifications** checkboxes and set the **On Modified** dropdown box to **Clean**

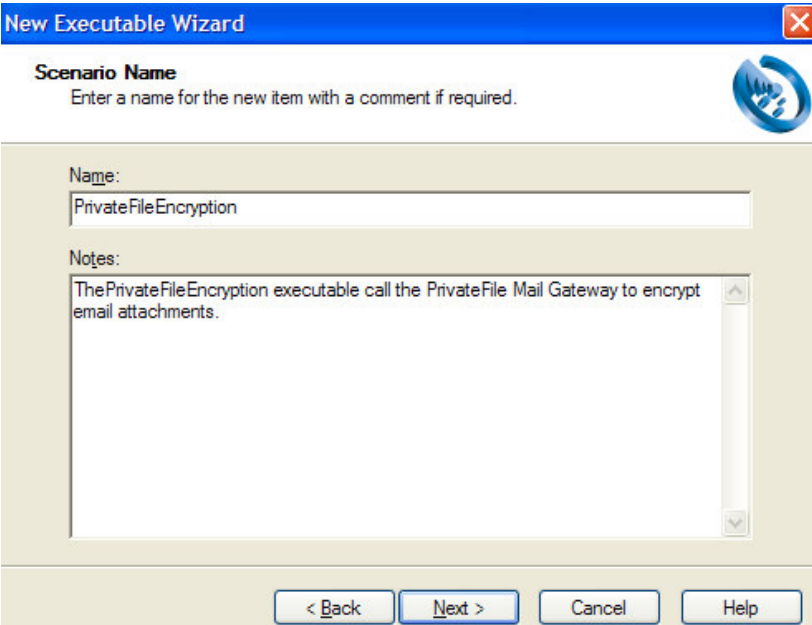


The screenshot shows the 'New Executable Wizard' dialog box with the 'Classifications' tab selected. The title bar reads 'New Executable Wizard'. Below the title bar, the section is titled 'Classifications' with a sub-instruction: 'Each unique outcome or result for a Scenario is called a Classification Type. For each type select a Classification or type the name of a new one.' There is a circular icon with a globe and a lock symbol. The main area contains the text 'For each possible scenario outcome, associate a classification.' followed by two checked checkboxes: 'Include System Classifications' and 'Include Inclusive Classifications'. Below these is a dropdown menu labeled 'On modified:' with 'Clean' selected. At the bottom, there is a yellow information box with a note: 'Note: Create a new Classification by typing the name directly into the appropriate edit field.' and four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Click **Next** to the **Scenario Name**

Enter **PrivateFileEncryption** in the **Name** field

Click **Next** to finish the creation

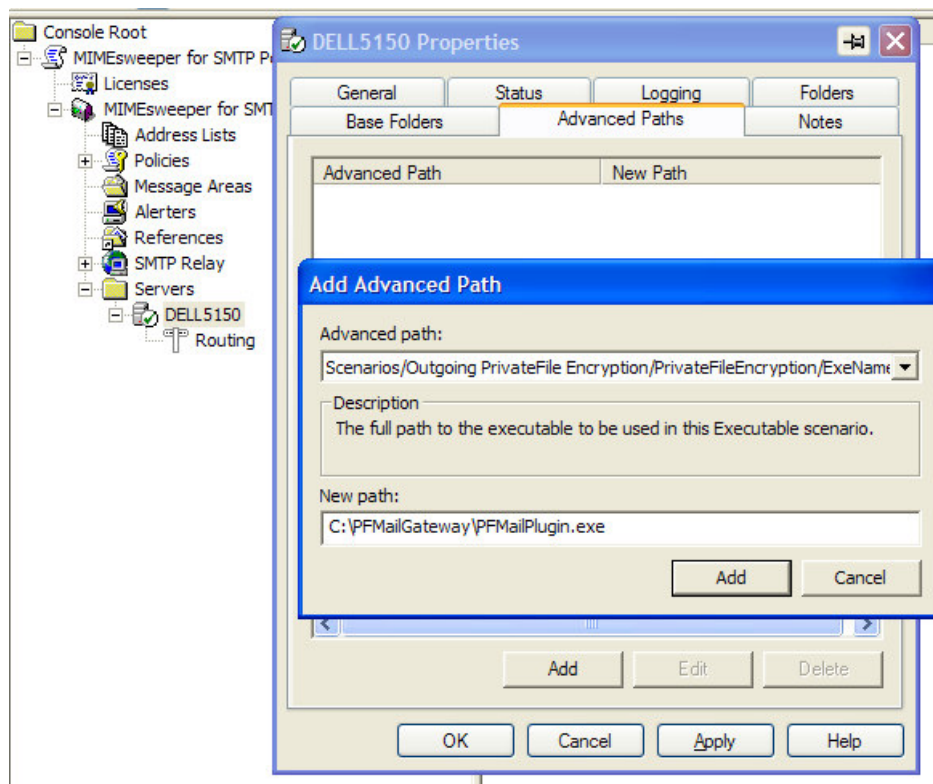


The screenshot shows the 'New Executable Wizard' dialog box with the 'Scenario Name' tab selected. The title bar reads 'New Executable Wizard'. Below the title bar, the section is titled 'Scenario Name' with a sub-instruction: 'Enter a name for the new item with a comment if required.' There is a circular icon with a globe and a lock symbol. The main area contains a text input field labeled 'Name:' with 'PrivateFileEncryption' entered. Below it is a text area labeled 'Notes:' containing the text 'ThePrivateFileEncryption executable call the PrivateFile Mail Gateway to encrypt email attachments.' At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

## Create AdvancedPath Entry

The **AdvancedPath** entry is setup to point to the exact path of the **PrivateFile Mail Gateway** executable.

In the **MIMESweeper for SMTP** select the **Servers** node. Right-Click on the server name and select the **Advanced Paths** tab and select **Add**




In the **Advanced Path** field enter  
**Scenarios/Outgoing PrivateFile Encryption/PrivateFileEncryption/ExeName**

In the **New Path** enter  
**C:\PFMailGateway\PFMailPlugin.exe**

Select **Add** to commit the new entry.

## Commit Configuration

Click the  button in the toolbar to save the configuration. Select **Yes** to apply the configuration after it has been saved

## PrivateFile Mail Gateway Setup

This section goes through the steps necessary in the **PrivateFile Mail Gateway** Administration function to setup a rule which encrypts all attachments going between **YourCompany.com** and **PrivateFile.Demo**

Open the Administration application using **C:\PFMailGateway\PFMailPluginAdmin.exe** and enter the password that you setup during installation. From the main screen choose **New...**

Enter a record as show. The **ID** is assigned automatically

This record specifies that all emails going from **joe@YourCompany.com** to **john@PrivateFile.Demo** will be encrypted using the encryption key **johnspassword**. The attachments will be encrypted as **PrivateFile Self-Decrypting executables**. This record is valid for **Outbound** emails.

Press **OK** to commit this change.

The screenshot shows the 'Edit Record' dialog box with the following fields and values:

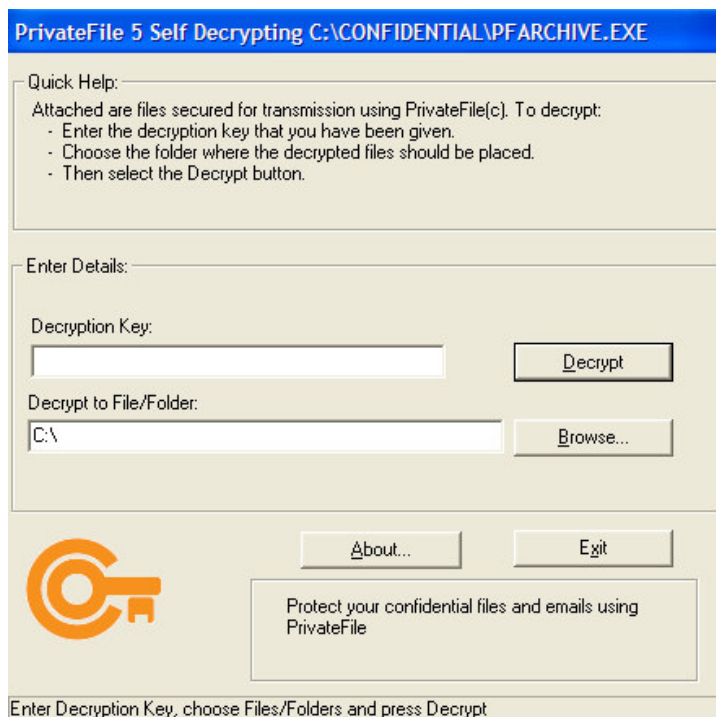
ID	6
From Name	joe
From Domain	YourCompany.com
To Name	john
To Domain	PrivateFile.Demo
Key/PGP Passphrase	johnspassword
Encryption Type	1 - Self Decrypting
In/Out	2 - Outbound and Inbound
Allow Personal Encryption	<input type="checkbox"/>
Local Contact	
Remote Contact	Please contact joe@yourcompany.com if you are having any issues.
Multiple Recipients Rule ID	<input type="checkbox"/>
Fallback Rule ID	<input type="checkbox"/>

Buttons: OK, Cancel

## Sending Emails

At this stage all the necessary configuration changes have been made to encrypt the emails going from joe@YourCompany.com to john@PrivateFile.Demo.

When [joe@YourCompany.com](mailto:joe@YourCompany.com) sends an email to a recipient at John@PrivateFile.Demo, the attachments will come through as an attachment entitled **PFarchive.exe**. This is a self-extracting executable. The recipient can open this and enter the encryption key **johnpassword** to decrypt the attachments.



## Other Options and Features

If the company **PrivateFile.Demo** has an equivalent infrastructure, then **PrivateFile Mail Gateway** can be setup to automatically decrypt the emails as they arrive in from **YourCompany.com**. In this way the encryption and decryption will be completely transparent to both sender and recipient.

**PrivateFile Mail Gateway** can be setup so that either only the attachments are encrypted or both the attachments and body of the email are encrypted. In the latter scenario, the body will be encrypted as a separate file and sent as an attachment.

**PrivateFile Mail Gateway** rules can be setup so that different encryption algorithms (e.g. SMIME encryption, PGP etc.) can be applied to different recipients. So for example, if **CompanyB.com** uses PGP then rules can be setup so that mails going to **CompanyB.com** will be encrypted using PGP.

## Contact Us

If you have any queries or simply want more information, do not hesitate to contact us:

Email: [info@private-file.com](mailto:info@private-file.com)

Tel: +353-1-6420550