

# Policy Management

Although they can vary widely in nature and degree, corporate policies exist to ensure a hostile-free, professional work environment. Modus™ helps enforce your email communications policies, protect your reputation and garner employee trust by analyzing email for personal health information, abusive and inappropriate content, proprietary information and forbidden attachments.

Through Vircom's Sieve implementation and other built-in settings, Modus' policy management allows:

- Management of File Attachments
- Policy enforcements
  - Proprietary information
  - Inappropriate content
  - Required Encryption
- eMail Flow Management
  - Communication control
  - eMail redirection
- Content-based archiving

The following paragraphs will describe how several of these management policies could be implemented. Examples are given to increase comprehension.

## ***Management of File Attachments***

### **Forbidden Attachment Option**

The forbidden attachments feature of ModusGate allows you to block attachment by name or type, preventing new types of viruses or unwanted content to enter your system.

Through this, you can build a list of attachments that will be automatically blocked by ModusGate. For instance, you may elect to automatically block .VBS files, typically carriers of viruses likely to infect users.

There are three levels of blocking for attachments in ModusGate:

- Normal,
- Strong,
- Extreme.

Would one mailbox be set at the "Strong" level, the modusGate will block all the attachments listed in the "Normal" and "Strong" lists. Only the attachments listed within the "Extreme" list will go through. So basically, the usual attachments (like DOC files) will be listed in "Extreme".

The level of scanning for forbidden attachments can be adjusted at system, domain and user level, and can be delegated to users or domain administrators.

The system also allows "Fingerprinting". Fingerprinting is a method by which the real attachment type of a specified file is detected. This prevents files from being sent through the engine being renamed. For instance, if Fingerprinting is enabled and MPG files are listed as forbidden attachments, the attachment scanner will block all MPG files, even if one is renamed SUSPICIOUS\_FILE.TXT.

Another option enables the attachment scanner to intercept all messages exceeding a specified size.

## Specific Attachment Rules

Through Sieve scripting, the modusGate can fine tune the attachment policy to more specific conditions.

### Example

System Administrators often protect mail servers after a Virus alert has been received from AV vendors and no solution has been found yet.

For instance let's say that the virus spreads in emails that have the following characteristics:

*Title is "Re: Your Order" or "Await your o.k."*

*The attachment is "payments.xls.exe" or "refund.pdf.exe"*

Then one could write the following blocking script:

```
if header :contains "subject" ["Re: Your Order", "Await your o.k."] {  
  if attachment :matches ["*payments.xls*", "*refund.pdf*"] {  
    discard; stop;  
  }  
}
```

## Policy Enforcements

### Ensure confidential information

A company may have a need to block users from sending attachments with certain names to the outside world.

For example, documents containing sensitive customer information, financial documents, etc... It is possible to accomplish this in a Sieve script by flagging certain attachment names.

### Example

Let's assume your own domain is widget.com and that the administrator wants to block, say, any attachment with the word "customer" in the filename ONLY if it's outbound (i.e.: not going to local domain). In other words, the administrator wants to block any email sent to a domain other than "widget.com" with a specific word "customer" somewhere in the attachment name.

Then, one would write the following script:

```
if not envelope :contains "to" "widget.com" {  
  if attachment :matches "*customer*" {  
    discard; stop;  
  }  
}
```

Continuing the example, let's say multiple possible filenames should also be caught. For example, "legal" as well...

The following script could then be used:

```
if not envelope :contains "to" "widget.com" {  
  if attachment :matches ["*customer*", "*legal*"] {  
    discard; stop;  
  }  
}
```

Remember that the Fingerprinting option is available to make sure that the Sieve scanner will block the confidential file, even if one has renamed the file GENERAL\_INFO.TXT.

## Ensure messages do not contain inappropriate content

As a company, one may want to block messages that contain inappropriate content (like abusive language) or confidential content that can only be sent from and to specific people (like Personal Health Information - PHI).

### Example

Let's say a company wants to block all messages containing sexually oriented words like "sex" and others. To remain polite, we will imagine these words being "Sex1", "Sex2" and "Sex3". Obviously we can have more than three words.

The following blocking script could then be used:

```
If anyof
  (header :contains "subject" ["sex1", "sex2", "sex3"],
   body :matches :text ["*sex1*", "*sex2*", "*sex3*"])
  { discard; stop; }
```

## Ensure messages are encrypted

Within some restricted research & development or human resource departments or within specific vertical markets (lawyers, healthcare, banking..) transmission of sensitive information may require encryption.

One may want to ensure emails within departments are encrypted, emails between specific people amongst departments are encrypted or that emails between specific people in a department and external partners are encrypted.

modusGate can block emails where header elements do not match specific rules. For instance, if the encrypted message has a header element like:

```
x-encryption: yes
```

then modusGate could block all messages that would not follow that header requirements.

### Example

For instance, let's say that one wants to force jimbob and joejob to only talk to each other in an encrypted fashion (their domain is widget.com), then one could write a script like this:

```
if envelope :contains "from" ["jimbob@widget.com", "joejob@widget.com"] {
  if envelope :contains "to" ["jimbob@widget.com", "joejob@widget.com"] {
    if not header :contains "x-encryption" "yes" {
      reject "Communication between jimbob & joejob must be encrypted";
      stop;
    }
  }
}
```

## ***eMail Flow Management***

### **Communication enforcement**

A company may have a need to block users from communicating amongst each other or from communicating to the outside world (using the email system just to communicate within the company).

While there is a broad range of Blacklist and Whitelist settings available in Modus that could answer these requests, some might be very specific and require a Sieve script.

#### Example

Let's say that a company does not want to have the people at the reception (from a company called Widget) sending emails to the outside world. Then we could write the following script:

```
if envelope :contains "from" ["reception1@widget.com",  
"reception2@widget.com"] {  
  if not envelope :contains "to" "widget.com" {  
    reject "External communication not allowed";  
    stop;  
  }  
}
```

### **eMail Redirection**

Based on some conditions, you can also redirect emails towards a specific email address.

#### Example

Let's imagine that a support organization wants to have all its engineers aware of a new entering call whoever it was directed to. Let's also imagine that all assigned calls have a specific ticket number mentioned in the title and that all support engineers are part of the "support" mailing list.

We could then write the following script:

```
if envelope :contains "to" ["engineer1@widget.com","engineer2@widget.com",  
"engineer3@widget.com", "engineer4@widget.com", "engineer5@widget.com"] {  
  if not header :contains "subject" "Ticket" {  
    redirect "support@widget.com";  
    keep;  
  }  
}
```

### **Content-based Archiving**

Based on some conditions, one can also archive emails in a specific folder.

#### Example

The following custom Sieve script can be used to make a copy of every email sent or received through Modus about a particular project. In the example, the project is question is "Project" and relates to a specific company "Company". The copy of the MSG file will be saved into a folder called "Project" in the "Company" sub-directory.

```
if anyof
  (header :matches ["subject"] ["*Customer*", "*legal*"],
   body :matches ["text/plain"] ["*Customer*", "legal*"]
  )
{ fileinto "c:\\Company\\Project"; keep; }
```

Note: Be careful to monitor the size of the "\\Company\\Projects" folder as message files could accumulate and fill the disk drive quickly.

## Sieve Script Overview

Please refer to the modusGate or modusMail manual for a full description of the Sieve commands.