



modusMail

NEW FEATURE
GUIDE
Version 5.0



Table of Contents

Overview	3
System Requirements	3
Policy Management	3
Securing the Interface	4
Creating Policies	5
Groups	5
Dictionaries	6
Policies	6
Content Conditions / Dictionaries	7
Message Handling	7
Priority / Policy Order	9
Administration Console Changes	9
Logging and Other Changes	10
Sender Reputation Service (SRS)	10
Scan Engine Changes and Improvements	11
Quarantine Delegation	11
Trusted Senders: Users Cannot Trust Own Addresses	12
Console RSS Feed	12

Overview

The following new features and enhancements have been added to modusMail 5.0:

- Policy Management
- SRS
- Scan Engine Changes and Improvements
 - Prevent users from trusting own addresses
- Quarantine delegation
- Console RSS Feed

System Requirements

The following are the recommended minimum system requirements for modusMail:

- 2.13 GHz Intel® Pentium® IV processor
- 40 GB (or higher), 7200 RPM hard drive (mirrored is recommended)
- 1024 MB RAM
- Microsoft® Windows Server 2003 or Server 2008 with the most recent Service Pack
- The system requires .NET 3.5 SP1 prior to installing the modus package
 - The Windows® Server version must be 2003 or above to support .NET 3.5.
 - Windows 2003 Web Edition is not supported

Windows Server Version Information:



1. As of modus 5.0, Windows Server 2000 is no longer supported.
2. 32-bit versus 64-bit platforms: Note that the core modusMail server component is a 32-bit application that can be installed and run on a 64-bit platform. However, the web components are not compatible with 64-bit and must therefore be installed on a separate Windows Server 2003

Policy Management

The modus™ Policy Management Edition is designed to help protect against data leakage of personal, financial or proprietary information through email. You can control what content can and cannot leave or enter your local system, and how that content will be treated.



You must be licensed to use Policy Management (PM). If PM access is added to your license key after installing 5.0, you must restart the following services to use the program: modusadm, moduscan and IIS.

Virus, attachment and regular spam scan controls (including custom rules) remain separate from PM to ensure continued operation with or without the module.

Virus and attachment scans continue to run first, prior to all other content rules.

Securing the Interface

Restrict Access to Specific Users

Policy Management is a web-based application and the WebPolicy virtual directory is created automatically in IIS during installation. The program uses Windows® authentication to determine who has access: by default, anyone with a valid account on the local domain can log into the program. Therefore you must restrict access by specifying the user or group of users who will be the policy administrators.

Built-in authorization settings define a group called *EmailPolicyAdministrators* (see the web.config file located in ...\\Vircom\Web\WebPolicy). Access to Policy Management must be limited to the users who are assigned as members of this group:

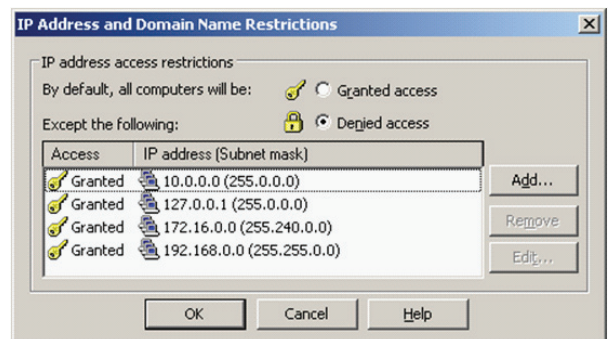
- Create a group called *EmailPolicyAdministrators* on your system and assign the designated users to this group
- Or, if the server is not configured as part of the domain, create *EmailPolicyAdministrators* as a local group on the modusMail server
 - Add the policy administrators as local users on the server
 - Add those users to the *EmailPolicyAdministrators* group

Restrict Access to Specific IPs

For additional security, the installer automatically attempts to restrict access to WebPolicy to internal IP address blocks only. If automatic setup is unsuccessful, or if you'd like to add/modify the addresses, follow this procedure:

IIS 6:

- Open **Internet Information Services (IIS) Manager**
- Locate the **WebPolicy** site (usually within the Default Web Site tree)
- Right-click to select **Properties**
- Select the *Directory Security* tab > *IP address and domain name restrictions*, and click **Edit**
- Select Denied access as the default setting and enter or modify the IPs to be allowed

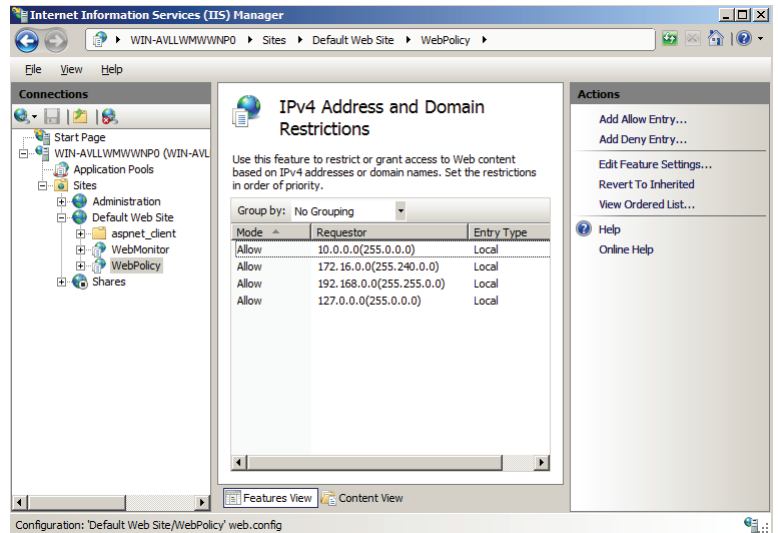


IIS 7 / Windows Server 2008 - Step 1:

- Open **Server Manager** and go to **Roles**
- Scroll down and click on *Add Role Services*
- Under **Security**, check *IP and Domain Restrictions*
- Click **Install**

Step 2:

- Open IIS
- Locate **WebPolicy**
- Right-click to select **Properties**
- Select *IPv4 Address and Domain Restrictions*
- Click on **Edit Feature Settings**
- Select **Deny** and click **OK**
- Click **Add Allow Entry** and enter the IPs to be allowed



Creating Policies

To access the interface, go to: <http://localhost/webpolicy>, or replace 'localhost' with your actual website name or IP address. The program supports Firefox, Chrome and Internet Explorer (version 7 and above).

To create a policy:

- Step 1: Create custom groups from local domains and mailboxes
- Step 2: Create your dictionaries (lists of terms), or import lists of terms. Note that dictionary content can also be created on the fly within the Policy screen
- Step 3: Begin creating the Policy: set the message content, handling rules and the groups or users to whom the policy will apply

Groups

To simplify the policy administration process, create custom groups containing local domain and/or mailbox names, to which policies will be applied:

Figure 1

- In the Groups table, click **Add** and select the **Custom Groups** tab
- Enter the desired group name and click **OK**

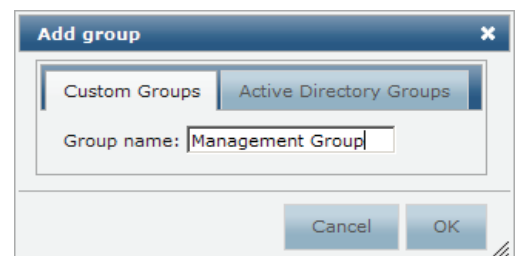
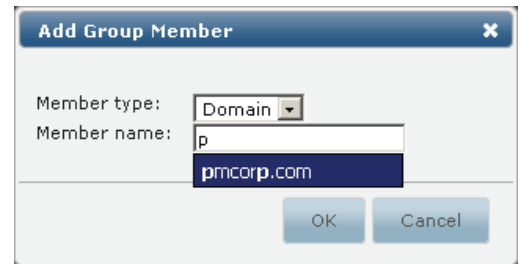


Figure 2

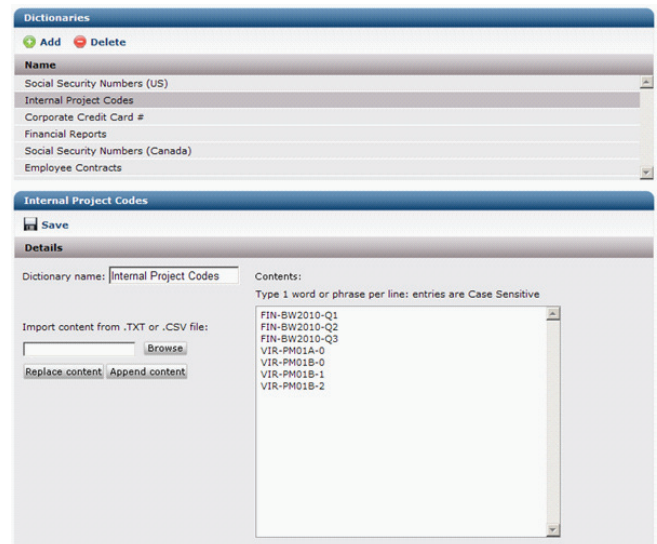
- In the *Group Members* table, click **Add**
- Select **Mailbox** or **Domain** from the *Member type* box and begin typing a name in the *Member name* box
- The system will auto-complete the list of names containing the letter(s) entered
- Select the desired name and click **OK** to save
- The group list can be viewed and selected from the *Policies* screen where policies are created



Dictionaryes

Dictionaryes, or lists of terms, are used to specify what message content will trigger a policy action. In the main Dictionaryes screen, you have the options to:

- Import lists of terms: these may be custom lists or commercially-available lists specific to your industry (e.g., tax and accounting terms, ICD medical codes and terms, etc.)
- Both text and CSV file formats are supported
- Create custom content by using the text editor. Note that Spell Check is supported by the edit screen.
- Only one word or phrase may be entered per line
- Entries are case sensitive, to help reduce the possibility of false positive results



The program also provides built-in dictionaryes containing Social Insurance/Social Security numbers, credit card numbers and international banking transit numbers (see **Policies - Content Conditions** for details). Only custom and imported dictionaryes are added to the table in the main Dictionaryes screen, but the entire list is visible when setting the content conditions in Policies.

Dictionaryes are stored within the ...**Vircom**\modusMail**Dictionary** folder. If you wish to edit the content, however, it should be done within the interface and not the file directly.

Policies

Policies are to be applied to local users, not to addresses external to your system. Policy scanning can be configured for inbound or outbound messages.

Inbound: i.e. the messages sent **TO** local mailboxes from external addresses

- Messages are treated according to content and handling rules applied to local recipients / group members
- All messages undergo regular virus, forbidden attachment and spam scanning prior to policy scanning

- Note that none of the regular virus, attachment, spam and phishing settings are included in Policy Management and must be configured separately
- Users' trusted lists are treated last in priority, to allow policies to take precedence over those settings

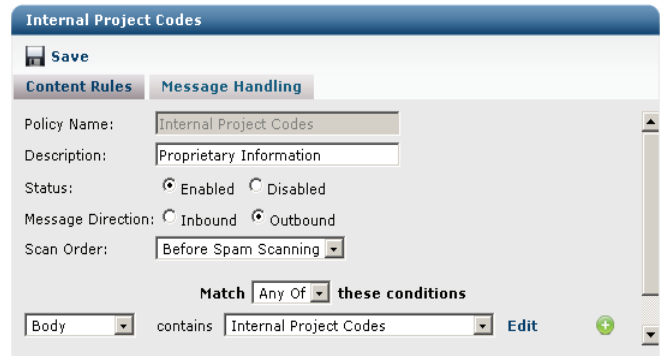
Outbound: i.e. the messages **FROM** local mailboxes to external addresses

- As above, messages are treated according to the content and handling rules imposed on local addresses
- Messages are scanned for viruses, forbidden attachments and spam prior to policy scanning
- Outbound scanning is the default option

Content Conditions / Dictionaries

Set the desired content conditions:

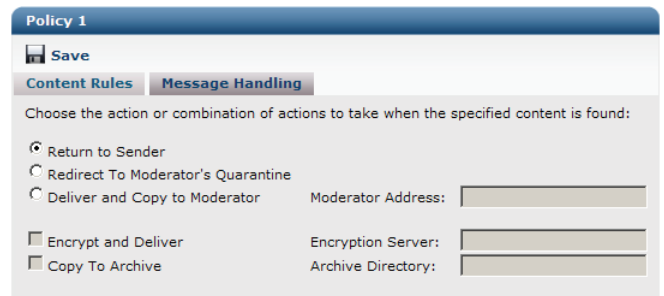
- **Any of** implies an 'or' condition, e.g. if the message contains A **or** B, then apply the rule
- **All of** implies an 'and' condition, e.g. if the message contains both A **and** B, then apply the rule
- Set the content rules
 - Select the portion of the message to be filtered: Body, Attachment, Subject. At present, the system is able to scan the content of Office 2007 Word and Excel files (.docx and .xlsx, respectively), but not PDF files
 - Select the dictionary (or list of terms) to specify what content to filter for
 - You may select from the dictionaries imported in the main Dictionaries screen, create custom content or use one of the following dictionaries included with the program:
 - > Social Insurance Number sequences (Canada)
 - > Social Security Number sequences (US)
 - > International social security numbers
 - > Standard credit card numbers (American Express, Discover, MasterCard and Visa)
 - > International bank transit numbers (ABA, Canadian, IBAN and SWIFT)



Message Handling

Choose from the following message handling options:

- Return to Sender: blocks (bounces) the message, which is returned as an attachment to a policy violation notice
 - This is the default setting when Outbound scanning is selected
 - It is available for Outbound policies only



- Moderator functions:
 - Redirect messages to a specific moderator’s mailbox
 - Deliver the message to the recipient and send a copy to the moderator
 - Different moderator addresses can be used for different policies, but only one address may be used at a time (i.e., 1 moderator per policy)
- Copy messages to a specific archive folder
 - The directory can be modified per policy
- Encrypt messages
 - Unavailable for Inbound policies (encryption requests are determined by the message sender)
 - Messages can only be encrypted for external delivery: the system does not natively support local-to-local encryption
 - Encryption methods will be determined by the settings configured in the Administration Console (PGP or other encryption server connection or TLS/SSL certificate) and the method used by the recipient
 - The system will attempt a connection to the encryption server first, but if no settings are found it will try the TLS settings
 - If the system attempts a TLS connection with a specific certificate but the recipient does not have the matching certificate, the transmission will fail and the sender will receive a delivery failure notice.

Allowed message handling combinations

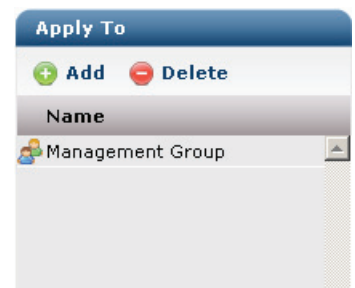
INBOUND	Audit	Archive	Encrypt
Return to sender: Unavailable	N/A	N/A	N/A
Redirect to moderator	√	√	N/A
Deliver and copy to moderator	√	√	√ (external address only)

OUTBOUND	Audit	Archive	Encrypt
Return to sender	√	N/A	N/A
Redirect to moderator	√	√	N/A
Deliver and copy to moderator	√	√	√ (external address only)

Apply the policy to specific groups/domains/users

After completing the policy structure, the Apply To section appears:

- Click **Add** to select the groups, domains and /or mailboxes for whom the policy will apply
- The system will auto-complete the list based on the information entered
- Select the desired name(s) and click **OK** to save
- The final step is to enable the policy



Moderator / Quarantine Functions

Messages flagged for the moderator are handled in the following manner:

- The subject line is tagged with “Approval Required: *Policy name* violated,” so the moderator can easily identify and filter these messages from their regular mail traffic
- The original message is attached to a notification: the moderator is able to see the message details such as the sender and recipient addresses, as well as the content.
 - The content of the notification message can be customized: go to the ...**Vircom\Web\WebPolicy\Locales** folder and open the subfolder that corresponds to your preferred language. Open the *strings.xml* file with Notepad and locate the **<ModeratorNotificationBody>** tag: enter your own text between the tags, close the file and restart the modusadm service.
- Messages redirected to the moderator are stored in a special folder within the quarantine
- These messages are included in the moderator’s quarantine report, in a separate Policy Violation section under a new Policy category
- The moderator can review the content and optionally release it to the original recipient
- Unlike other quarantined content, policy violating messages are not deleted automatically in the event that the content must be preserved. These messages can be moved to an archive directory or manually deleted, if not required.

Priority / Policy Order

- **To prevent data leakage, the most restrictive policies should be given the highest priority.**
- Policies are applied in the order in which they are listed
- Priority can be changed by moving policies up or down in the list
- If, however, an exception is required, the exception should be listed first

Scenario:

- Policy 1 blocks the sending of financial information and applies to all staff
- Policy 2 stipulates that the President, the CEO and the Accountant are allowed to send financial information but it must be encrypted
- If those 3 people absolutely must be allowed to send that information, the second policy should be placed first in the list

Administration Console Changes

- A new Policy category has been added to the scan engine to identify and filter the messages that trigger a policy.
- A Policy tab has been added to the Quarantine screen, to display the list of messages that trigger policies
- Policy has also been added to the **Quarantine > Find** functions to enable the search mechanism
- A new service has been added to the **System > Services** list: the Mail Server Configuration Service (MODUSCF). This service is used to manage group information and will be visible no matter whether Policy Management is activated or not.

Logging and Other Changes

Audit Log

Policy violating messages are recorded in the Audit Log (if Audit is enabled). These messages can be searched using the new Policy Violation option in the **Scan Results** dropdown list.

Operations Log

Policy scan results are recorded in the Operations (OPR) log and specify the name of the policy that is applied and the action taken.

Messages set to be returned to sender are reported as “rejected” in the log:

```
The file C:\Vircom\modusMail\spool\invirus\B00\0000\B0000000111.MSG is being scanned for policies.
---- MODUSCAN log entry made at 06/02/2010 16:16:20
The file C:\Vircom\modusMail\spool\invirus\B00\0000\B0000000111.MSG has been scanned and has been rejected by the script
: "Social Media" <5>.
```

Messages flagged for moderation are reported as “discarded” in the logs. ‘Discard’ means the message was quarantined, not deleted:

```
The file C:\Vircom\modusMail\spool\Policy\B00\0000\B0000000114.MSG has been created for detection of Message
B0000000113.MSG.
---- MODUSCAN log entry made at 06/02/2010 16:34:04
The file C:\Vircom\modusMail\spool\invirus\B00\0000\B0000000113.MSG has been scanned and has been discarded by the
script : "Offensive words" <0>.
```

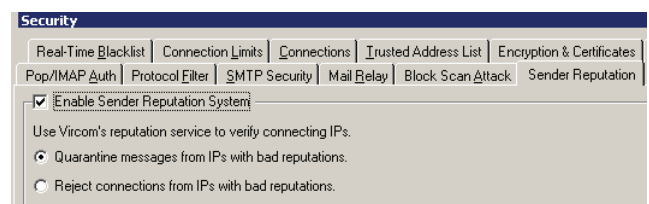
File Storage

- Policies are stored in the Sieve database within the *dbo.SieveCatalog* table
- Dictionaries (including custom and those supplied by the system) are stored in the *...\Vircom\modusMail\Dictionary* folder

Sender Reputation Service (SRS)

Vircom has enhanced the performance of its SRS server to help reduce traffic from IPs with bad reputations. The IP lists are updated frequently and are more reactive than standard RBLs. If a spam wave from a new source of IPs is detected, for example, clients are quickly protected from that wave if they begin receiving messages from the same IP source. Similarly, if a computer is removed from a blacklist or botnet network, its IP is quickly removed from the SRS list.

Configuration options include blocking bad IPs at connection, or quarantining the messages. This feature is disabled by default.



Message Details

Quarantined messages are included in the spam list and logged in the Operations (OPR) log, while blocked messages are logged in the Error (ERR log). Both log entries display the SRS server connection (reputation.vircom.com).

The following is a sample message header from a SRS-quarantined message:

```
Received: from MODUSCAN (SERVER.vircom.com [192.168.X.X] bySERVER.vircom.com(modusMail SMTPDS 5.0.911.0) with FILECOPY
id<F0317868152@server.testdomain.com>;Tue, 11 May 2010 11:57:40 -0400
Message-ID: <F0317868152@server.testdomain.com>
From: "Cleo Charlie" <john@moo.com>
Subject: Oh hello, have you finished??
To: <moo@moo.com>
Reply-To: "Cleo Charlie" <john@moo.com>
X-Modus-Audit: FALSE;0;0;0
X-ModusMail-Sieve: "\Miscellaneous\Normal" <0>
X-Spam: [SRSRBLMODUS,0,41]"\Miscellaneous\Normal" <0>
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="=_Part_c196d886_07ab_4607_a72a_534fd38806d4"
```

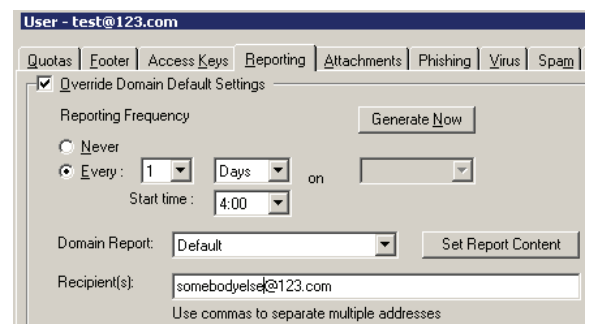
Scan Engine Changes and Improvements

Quarantine Delegation

Quarantine reports can now be delegated to a specified address (or multiple addresses) to provide quarantine management on behalf of the mailbox owner. At present, this feature can only be configured in the console (in **Users > Preferences > Reporting** settings).

Scenario:

- The Boss wants his Administrative Assistant to be able to review and manage his quarantine contents for him
- The Assistant's email address is entered into the Boss' Recipients list in his Reporting settings
- The Assistant then receives copies of the Boss' Quarantine Report and can either delete or release messages, or trust the sender's address without having to log into the Boss' quarantine settings



Trusted Senders: Users Cannot Trust Own Addresses

The system now automatically prevents users from trusting or whitelisting their own email addresses in an attempt to bypass spam scanning. This feature provides security in the event that a spammer breaks into a local account to send messages, or attempts to spoof local addresses.

If both the sender and recipient addresses match, the message undergoes regular spam scanning, irrespective of what is displayed in the user's mailbox settings in the Administration console or Web Quarantine screen. (In other words, end users will not be able to see that they are being prevented from trusting their own addresses.)

For security purposes, this feature is enabled by default but can be disabled, if required, in the registry. To turn this feature off:

- Go to **HKLM\Software\Vircom\VopMail**
- Create a REG_DWORD called AutoTrustedSelfCheckSwitch
- Set the value to 0 and restart the moduscan service
- Setting the value to 1 will re-enable the feature

Console RSS Feed

An RSS news feed window has been added to the Administration Console. It will be used periodically to provide notification of the availability of new releases, updates or new features (such as Policy Management).

To dismiss the current message, simply click **Close**: it will only reappear in the event of a new notification.

