



# Release Notes

Version 4.3



Urgent Existing Custom Theme Consideration for WebQuarantine.....	4
Screen Resolution .....	4
New Features .....	4
New WebMonitor application .....	4
Login .....	4
System Health View.....	4
Trend Graph display .....	5
Activity Gauges.....	5
Gauge Increments .....	6
Service Status.....	6
Performance Profile .....	6
Modus Version Information.....	6
Mail Traffic .....	7
Modus MIB and SNMP Counters .....	8
SURBL .....	10
Archive Scanning.....	11
Enforcement of Corporate Email Policies (includes Parental control).....	11
Scanning Sequence.....	12
Creating Policy Scripts.....	13
Spam confidence levels added to Quarantine Report.....	14
Modus Database Changes.....	15
Modus Database Scripts .....	15
PostgreSQL Configuration Option .....	15
Quarantine Database.....	16
SQL Quarantine Database Script .....	16
Monitoring Database .....	17
PostgreSQL Monitoring.....	17
MSSQL Monitoring.....	18
Extended Database .....	18
MSSQL Extended database.....	18
SieveStore Database .....	19
MSSQL SieveStore Database (New Installs ONLY).....	19
Blacklist/Whitelist import tool available.....	20

New features .....	21
Quarantine Search.....	21
Resizable text and 800X600 support.....	21
Message headers .....	21
Persist Sorting Order.....	21
Mailbox statistics .....	22
Foreign Language Support .....	22
Domain customization.....	22
WebQuarantine Known Issue .....	22
WebQuarantine 4.3 Interface Customization .....	23
Browser Compatibility for WebQuarantine .....	23
Custom.Config Basic Functionality Customization .....	23
Logos.....	24
Custom Login page or Portal Integration.....	25
Theme Customization.....	25
Changing the Login page color:.....	26
Changing the Top Menu color:.....	26
Changing the lists hover color: .....	26
Changing the background color of all panels: .....	27
Removing Statistics (or other major menu items).....	28
Hiding a section of the settings: .....	28
To hide the options section:.....	28
To hide the email filtering section:.....	28
To hide the user contact information section:.....	29
To hide the rules section:.....	29
To hide the auto-reply section: .....	29
To hide the external accounts section:.....	29
To hide the aliases section: .....	30
To hide the Server Blocked/Trusted list from the Settings page: .....	30
WebQuarantine Message Customization .....	31
Changing default strings.....	31
Bug Fixes .....	32
Known Issues.....	33

## **Urgent Existing Custom Theme Consideration for WebQuarantine**

If you had customized the 4.0/3.x interface and want to continue using it, you will have to redirect the webmail path in IIS to point to your original folder. The previous webmail folder that you've been using will be renamed to Pre43Webmail.

Please note also, the much older 3.x Modus Webmail application is no longer packaged and supported, and if you're using this, it will remain unchanged by a Modus install EXCEPT that the URL path for your users will change (as described above).

## **Screen Resolution**

For best performance, the Modus console requires a minimum screen resolution of 1024 X 768.

## **New Features**

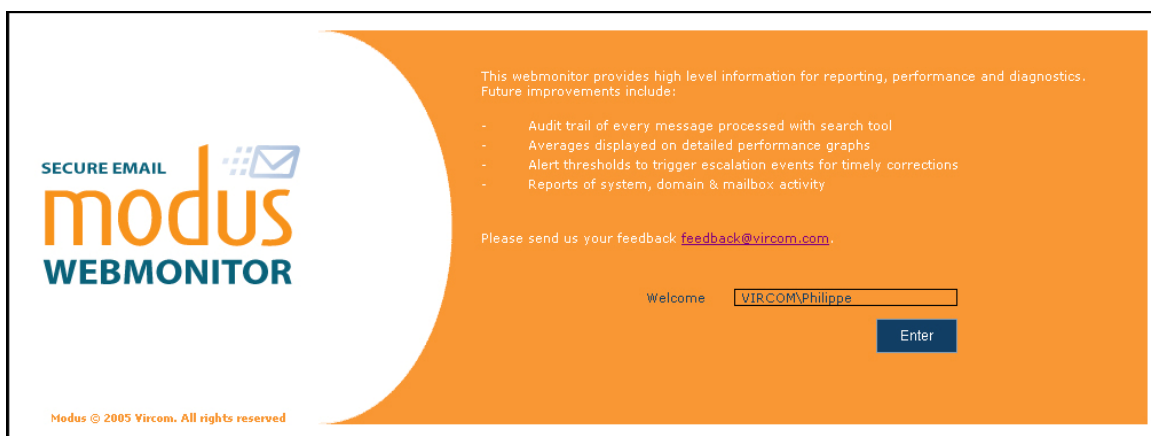
### **New WebMonitor application**

The new WebMonitor application contains information about system health, and the mail statistics provided by the old webmonitor under the menu item "Mail Traffic". This application only runs in Internet Explorer 6.0 and we strongly recommend that you do not access it directly on the Modus server because it will interfere with Modus performance.

You will also need an SVG viewer in order to use the interface. You can download the SVG viewer from: <http://www.adobe.com/svg/viewer/install/main.html>

## **Login**

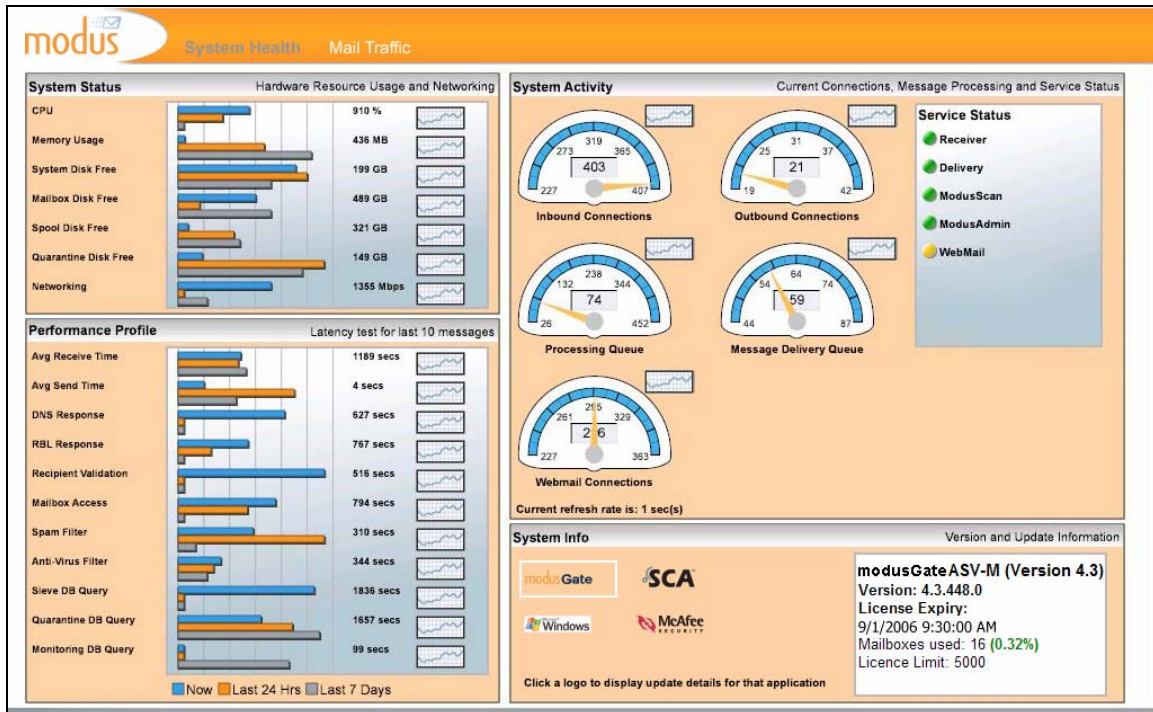
The application uses NT authentication, so your valid NT account must have permissions to access the folder where WebMonitor is stored to be able to login (the default folder would be c:\program files\vircom\web\webmonitor\). To access the application, open a browser window, enter your server's URL and type "/webmonitor/login.aspx" after the URL <serveraddress/webmonitor/login.aspx>



## **System Health View**

The new Modus System Health screen will show you information about:

- System Status (for the hardware Modus uses and interacts with). Click a trend graph icon to see performance trend graphs for the last hour, last 24 hours and the last week.
- System Activity (for Inbound and Outbound connections, Processing and Message Delivery queues, WebQuarantine Connections).
- Performance Averages (average performance rates for messages processed in the last second)
- Version Information (for Modus, your operating system, and about updates for your anti-spam/anti-virus engines)



### Trend Graph display

For the display of trend graphs, there will be three graphs:

1. *last hour*: average of readings at 20-second intervals
2. *last 24hrs*: average of readings at 8-minute intervals
3. *last week*: average readings at hourly intervals

### Activity Gauges

The activity gauges give a reading of the number of connections, or messages being processed, or the number of messages in the delivery queue at the time of reading. Since the page refreshes each second, the gauges will be displaying the precise number of each of the graphs each time the system reads the meters (once every second).

## Gauge Increments

The increments for the gauges will be determined dynamically and always in round numbers (either 10, 100 or 1000 depending on the amount of traffic experienced by the system). The lower threshold will be the rounded down lowest number of activity experienced by the system in the last 24 hours and the highest threshold will be rounded up to the highest number of activity experienced in the last 24 hours.

For example, if in the last 24 hours the lowest number of inbound connections had been 9 and the highest number of inbound connections had been 367, the Inbound Connections activity gauge increments would be between 0 and 400. So a user reading the gauge would know that if the arrow is straight up, they are receiving the average number of Inbound connections of the last 24 hours. If the arrow is leaning to the right, they would be experiencing a higher than average load. If the arrow was leaning on the left, they would be experiencing a lower than average load.

## Service Status

Green – service is up running

Orange – the service is either starting or stopping (you need to check in Windows services manager to verify the state of the service)

Red – service is stopped

NOTE: a service might stop and start itself automatically because of updates.

## Performance Profile

Modus measures average component performance for the delivery/processing time of messages passing through the system in the last second.

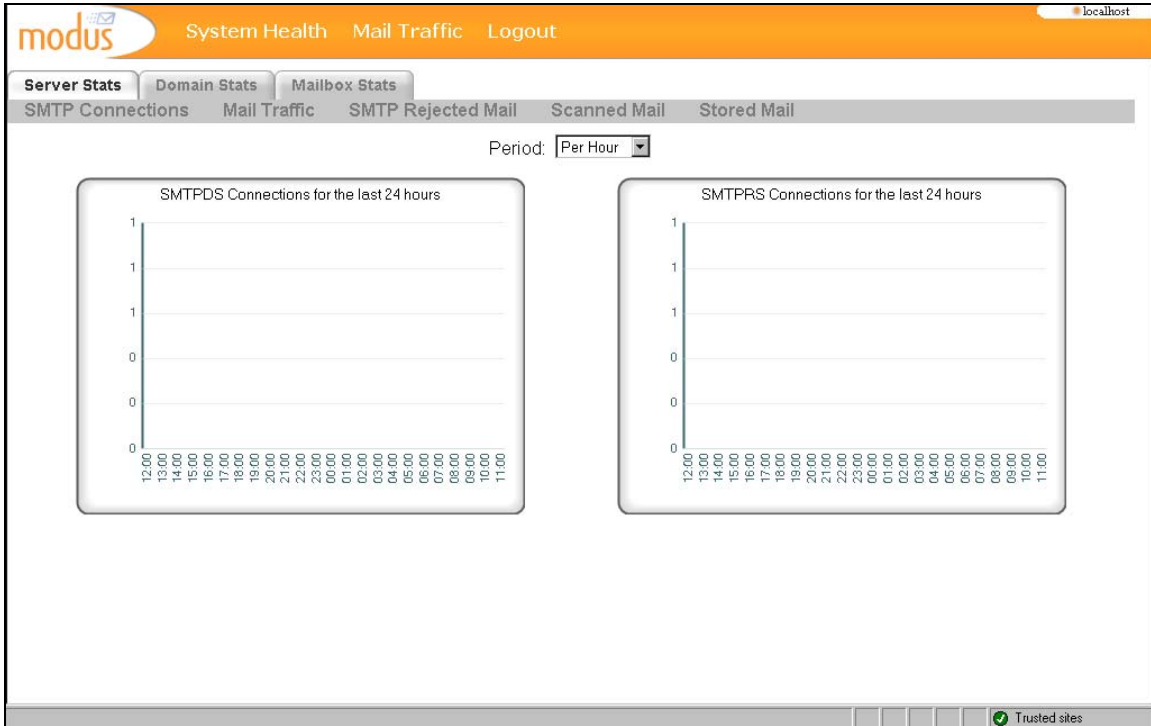
NOTE: if no messages were processed in the last second, the values will be zero – this doesn't mean that your system has a problem, simply that it was not required to perform in the last second. This could be true of some components in the message delivery process which were not required to process the particular messages in the system during the last second.

## Modus Version Information

- Modus version
- Spam engine, date of engine
- Result and date/time of last SCA engine update attempt (successful or failed)
- Anti-Virus engine (where applicable)
- Engine and Sequence number plus date of sequence number
- Result and date/time of last anti-virus update attempt (successful or failed)
- Operating System name and version, date/time of last reboot
- SieveStore, Quarantine and Monitoring DB types and versions

### Mail Traffic

The statistics provided by the old Modus webmonitor application are all still available – but now you can reference them by selecting “Mail Traffic” from the menu in the new WebMonitor application.



### **Modus MIB and SNMP Counters**

Modus can provide essential performance information about its activities for those companies who use a centralized system to monitor the performance of their network devices. Modus provides Simple Network Management Protocol counter values (SNMP counters) and the Modus Management Information Base (MIB). The Modus MIB is called VIRCOM-MONITOR\_Gate.mib and is installed in the main ModusGate directory.

Here is a table of all of ModusGate's SNMP counters.

<b>SNMP Counter</b>	<b>Counter description</b>
cpuProcessorTime OBJECT-TYPE	Current percentage of processor time used.
memoryCommitted OBJECT-TYPE	Current memory committed in bytes.
memoryCommitLimit OBJECT-TYPE	Memory commit limit in bytes.
smtprsActiveConnectionsIn OBJECT-TYPE	Current SMTP reception service number of active connections in.
smtprsClearActiveConnectionsIn OBJECT-TYPE	Current SMTP reception service number of active clear connections in.
smtprsEncryptedActiveConnectionsIn OBJECT-TYPE	Current SMTP reception service number of active encrypted connections in.
smtprsInvirusMessagesIn OBJECT-TYPE	Current SMTP reception service number of invirus messages in.
smtprsAverageReceiveTime OBJECT-TYPE	The time needed to receive a message on average (ms).
smtprsRblResponse OBJECT-TYPE	Average time a RBL request takes to complete (ms).
smtprsRelayAuthTime OBJECT-TYPE	Average time taken by a relay authentication request (ms).
modusScanInvirusMessagesOut OBJECT-TYPE	Current Scan service number of invirus messages out.
modusScanIncomingMessagesIn OBJECT-TYPE	Current Scan service number of incoming messages in.
modusScanSpamMessagesIn OBJECT-TYPE	Current Scan service number of spam messages in.
modusScanSpamScanTime OBJECT-TYPE	Average time taken to scan for spam (ms).
modusScanVirusScanTime OBJECT-TYPE	Average time taken to scan for viruses (ms).
modusScanSieveDbTime OBJECT-TYPE	Average time taken to access the Sieve DB (ms).
smtpdsActiveConnectionsOut OBJECT-TYPE	Current SMTP delivery service number of active connections out.

<b>SNMP Counter</b>	<b>Counter description</b>
smtpdsClearActiveConnectionsOut OBJECT-TYPE	Current SMTP delivery service number of active clear connections out.
smtpdsEncryptedActiveConnectionsOut OBJECT-TYPE	Current SMTP delivery service number of active encrypted connections out.
smtpdsAverageSendTime OBJECT-TYPE	The time needed to send a message on average (ms).
smtpdsIncomingMessagesOut OBJECT-TYPE	Current SMTP delivery service number of incoming messages out.
smtpdsHoldingMessagesIn OBJECT-TYPE	Current SMTP delivery service number of holding messages out.
smtpdsHoldingMessagesOut OBJECT-TYPE	Current SMTP delivery service number of holding messages out.
modusAdmSpamMessagesOut OBJECT-TYPE	Current Adm service number of spam messages out.
modusAdmProcessingQueue OBJECT-TYPE	Number of messages in transit or being processed.
modusAdmMessageDeliveryQueue OBJECT-TYPE	Number of messages queued for outbound delivery.
modusAdmSystemDiskFree OBJECT-TYPE	The amount of free space left on the device holding the server data.
modusAdmMailboxDiskFree OBJECT-TYPE	The amount of free space left on the device holding the mailboxes.
modusAdmSpoolDiskFree OBJECT-TYPE	The amount of free space left on the device holding the spool.
modusAdmQuarantineDiskFree OBJECT-TYPE	The amount of free space left on the device holding the quarantined messages.
modusAdmNetworkUsage OBJECT-TYPE	Network interface usage for all interfaces (bytes/sec).
modusAdmDnsResponse OBJECT-TYPE	Average time a DNS request takes to complete (ms).
modusAdmMailboxAccess OBJECT-TYPE	Average time taken to access the properties of a mailbox (ms).
modusAdmQuarantineDbTime OBJECT-TYPE	Average time taken to execute statements in the Quarantine database (ms).
modusWebMailSvrCurrentSessions OBJECT-TYPE	Current WebMail server number of sessions.
vircomMonitorServiceTable OBJECT-	The table holding information specific to

SNMP Counter	Counter description
TYPE	Monitor service.
vircomMonitorServiceEntry OBJECT-TYPE	The entry holding information specific to Monitor service.
modusMonitorDbTime OBJECT-TYPE	Average time taken to execute statements in the Monitor database (ms).

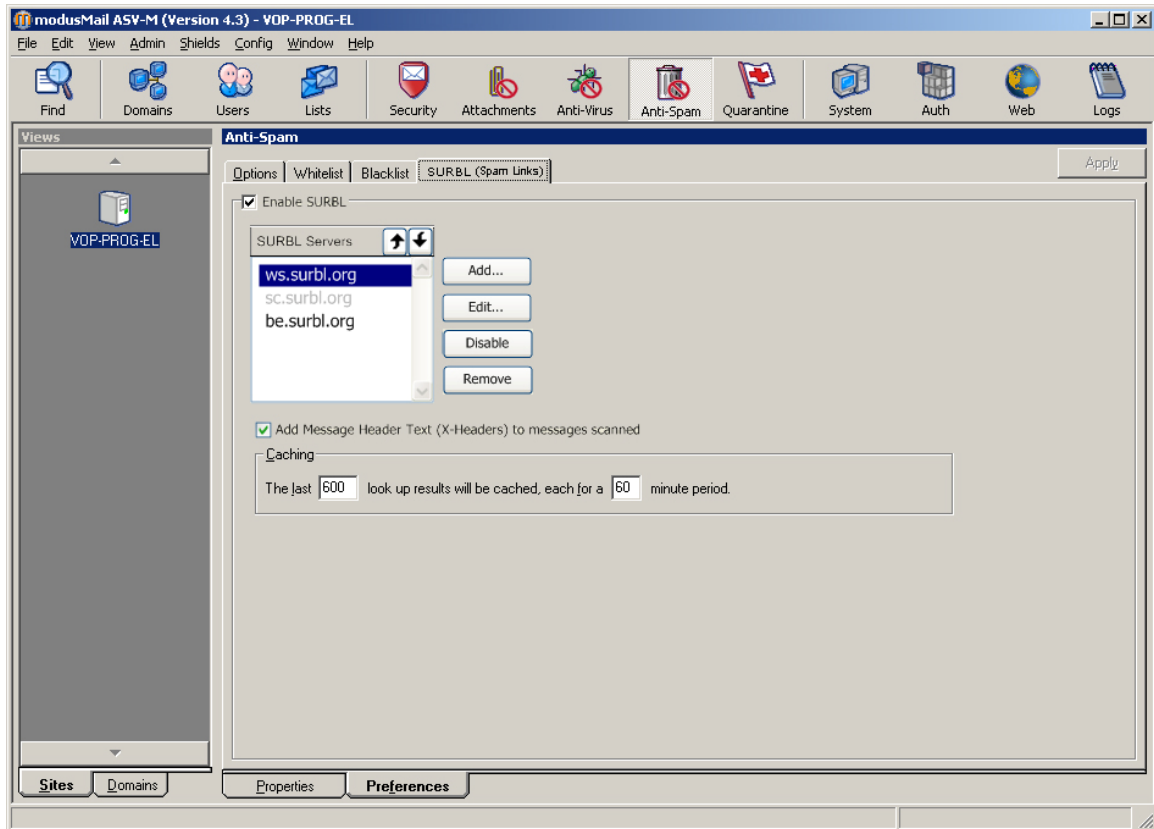
**SURBL**

SURBL is an RBL designed to be used to block or tag spam based on URLs (usually their domain names) contained within the body of the message.

Vircom recommends multi.surbl.org - please go to [www.surbl.org](http://www.surbl.org) for more information about SURBLs and for details about what the multi.surble.org list covers.

1. Go to **Anti-Spam > Preferences > SURBL (Spam Links)**
2. Click Enable **SURBL**
3. Click **Add** and enter the SURBL server(s) you want to use
4. Click **Apply**

Lookup of an email’s URLs will be performed randomly – not in order from beginning or end in case spammers bracket spam links in the list with legitimate links at either end of the list.



*NOTE: mockup displays ModusMail, but this feature applies to both ModusMail and ModusGate*

## Archive Scanning

Scan for forbidden attachments in compressed files (archives) – meaning a zipped message will be scanned not only for viruses (an old feature for Modus) but now for forbidden attachments (FAs) as well.

Go to **Attachments > Preferences > Options** to enable the feature for the system (this is a system-wide setting only).

## Enforcement of Corporate Email Policies (includes Parental control)

We have optimized our receiving service to be able to target mail traveling in specific directions so that you can customize sieve filters to be selectively applied to mail. An attribute is now added to the envelope (.rcp file) of a message to identify it as either:

From Outside to Outside = **Routing**

From Outside to Inside = **Incoming**

From Inside to Inside = **Local**

From Inside to Outside = **Outgoing**

A new feature that can be used either as a parental control mechanism or a communications policy for companies is that you can forward spam to another quarantine while preserving header information.

*NOTE: For this first release of the feature, we are reviewing the best way to implement it. For the policy/parental control scripts to be effective, they must bypass the trusted lists – so setting the scanning sequence to “Before all scanning” will take care of that. BUT if the script says “stop” (see examples following), this means that if the script is run and it catches messages that match its criteria, then the caught messages will not be scanned for viruses. Alternatively, if you set the scanning sequence for the script to after any of the content scanning, then some messages may bypass the script because of the trusted list.*

*Also, because order of processing is important in the custom filter lists (the first script is run first and so on down the list), the control script should be run last so that all other junk doesn't end up in the reviewer's mailbox.*

*Please send us your feedback about this feature.*

Sample CORPORATE control scripts:

```
if not envelope :matches "X-Sieve-Moderate" "*" {
  if header :contains "to" "suspiciousstaff@domain.com" {
    if header :contains "subject" "job offers" {
      x_moderate "moderate@mydomain.com";

      /* Send alert */
      x_mailer "moderate@mydomain.com" "alerter@mydomain.com" text:
        Subject: You have mail waiting your approval
        Please check your QT.
      .
      ;
      stop;
    }
  }
}
```

```
if not envelope :matches "X-Sieve-Moderate" "*" {
  if envelope :contains "Local-Status" "outbound" {
    if body :raw :contains "source code v1.0" {
      x_moderate "moderate@mydomain.com";

      /* Send alert */
      x_mailer "moderate@mydomain.com" "alerter@mydomain.com" text:
        Subject: You have mail waiting your approval
        Please check your QT.
      ;
    }
  }
}
```

Sample PARENTAL control script:

```
if not envelope :matches "X-Sieve-Moderate" "*" {
  if header :contains "subject" ["chatroom","singles"] {
    x_moderate "moderate@mydomain.com";

    /* Send alert */
    x_mailer "moderate@mydomain.com" "alerter@mydomain.com" text:
      Subject: You have mail waiting your approval
      Please check your QT.
    ;
  }
}
```

Explanation:

When a message meets the filter criteria, it will be quarantined in the account specified in the `x_moderate` line. This should be an account used solely for the moderation purpose so that the messages don't get lost among all the other quarantined junk.

The alert portion of the script is optional. When a message is filtered, an alert notice can be sent to the second address in the `x_mailer` line (e.g. `alerter@mydomain.com`).

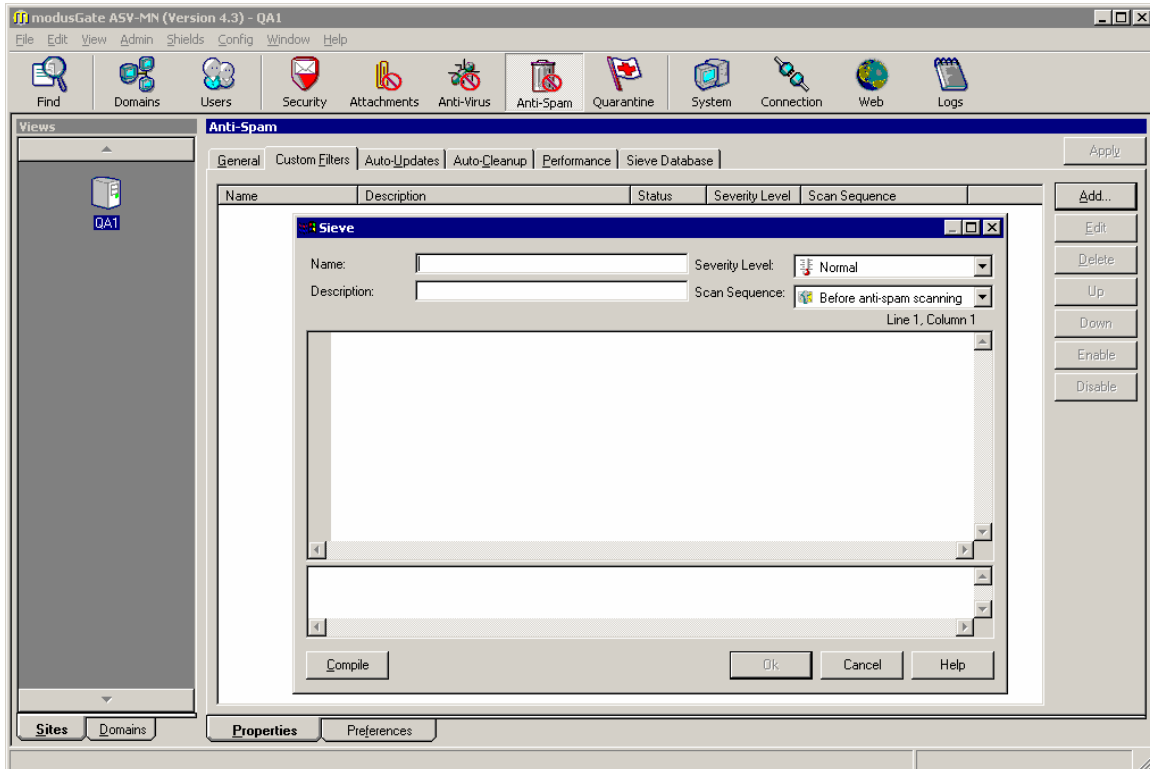
In the Administration console's Quarantine view, these messages will be tagged "[Requires Your Approval]" in the subject field. The WebQuarantine view will display the subject specified in the script, e.g. "You have mail waiting your approval."

The moderator will be able to release the message, and it will be delivered to the original recipient(s) with an additional header of "X-Sieve-Moderate".

## Scanning Sequence

Once you have created your policy scripts, you can choose when in the message processing sequence you want to run your scripts:

- *Before content scanning* (after the security checks are passed and the message is accepted for processing, but before anti-virus scanning begins)
- *Before anti-spam scanning* (after the anti-virus scanning is complete)
- *After all scanning* (run policy scripts last after the message has passed security, anti-virus and anti-spam scanning)



## Creating Policy Scripts

1. Go to **Anti-Spam>Properties>Custom Filters** in the Modus Console
2. Click **Add**
3. Enter a name, description and your custom script
4. Choose a severity level (works like the anti-spam severity levels – if set to “Normal” severity which is the default, the script will apply to everyone)  
NOTE: your anti-spam severity settings will determine what levels of policy scripts are applied in the system.
5. Choose the point in the message scanning sequence where you want your script to be run, either:
  - Before content scanning
  - Before anti-spam scanning (this is the default setting)
  - After all scanning
6. Click **Compile** to verify the integrity of your script, and then click **Apply**

***Spam confidence levels added to Quarantine Report***

Confidence level column added to quarantine report: messages rated High, Medium, Low depending on the quarantine level that trapped it (e.g. Normal=High, Strong=Medium, Extreme=Low)

## Modus Database Changes

For version 4.3 of Modus, we have made some changes to the Modus databases that you can choose to use depending on the database format you're using, or not at all if you want easy backwards compatibility.

You can use PostgreSQL for your Monitoring database, but for users upgrading to version 4.3 who have been using Microsoft Access you won't be required to change your database format unless you have performance reasons for doing so. *Please note that if you change the database format, you will not have your historical data. If you need to keep your historical data (Quarantine contents, SieveStore etc) we recommend that you do not change your database format until Modus 4.4 is released. As a rule, with the instructions below, existing customers should never run a script that ends with "new" because they will lose their data.*

For version 4.4 we will have a database administration tool that will allow you to convert your database format from:

- Access to either PostgreSQL or MSSQL
- PostgreSQL to MSSQL
- MSSQL to PostgreSQL

*Please note also that from version 4.4 onwards you will HAVE to use either PostgreSQL or MSSQL because Modus will no longer support Microsoft Access.*

## Modus Database Scripts

Modus contains the scripts described in the procedures in this section in the following directory structure:

```

...Vircom\ModusMail\DBStructures
    |-- PostgreSQL
    |     |-- Monitoring
    |
    |-- SQL Server
    |     |-- ExtendedDB
    |     |-- Monitoring
    |     |-- Quarantine
    |     |-- SieveStore

```

## PostgreSQL Configuration Option

The way Modus interacts with PostgreSQL databases is that data to be written to the database is cached to a log file until enough data has been accumulated for a disk-write to be warranted. Ideally, the log-size should be larger than the default setting because this allows Modus to perform faster (if PostgreSQL is writing to the disk too often it slows down Modus' performance).

The configuration setting "checkpoint\_segments" specifies when PostgreSQL can write data to the disk. PostgreSQL has two settings for the checkpoints. The first, checkpoint\_segments, is based on the amount of data modified. The other setting "checkpoint\_timeout" is a timeout in seconds, so if there were no checkpoints in the last X seconds, PostgreSQL will do one.

A segment represents a certain amount of data modified. The default value when PostgreSQL is installed is “3” meaning that when 3 segments of data are accumulated, PostgreSQL writes to the disk.

We recommend changing the `checkpoint_segments` value to 10 for optimum Modus performance (you can leave the `checkpoint_timeout` default value as is).

To change this setting:

1. Go to **Start > Programs > PostgreSQL > Configuration files > edit postgresql.conf**
2. Find the line `checkpoint_segments` and change the value to 10
3. Remove the `#` at the start of the line to uncomment the line
4. Save the file
5. Stop and start the postgresql server

### **Quarantine Database**

If you are using MSSQL for your Quarantine database, you will be able to allow your users to access their quarantine contents from their mail clients. We have provided a script that you can run on your database that will allow your users to access their quarantine contents from Outlook or whatever mail client they are using. (Please note, we have a script you can use to create a PostgreSQL Quarantine Database that also allows users to access their quarantine spam contents from their mail clients – please contact Vircom Technical Support for more information.)

### **SQL Quarantine Database Script**

1. Open the MSSQL Enterprise Manager, and either:
  - a. Create the database or use an existing one
2. Go to ...Vircom\ModusProduct\DBStructures\SQL Server\Quarantine to locate the the MSSQL script (`mssql_quarantine_without_imap.sql`) to create the tables
  - a. Open MSSQL Query Analyzer and run the script “`mssql_quarantine_imap.sql`”
3. Create the ODBC connection
4. Open the Modus console and go to **System > Quarantine Database**
5. Enter your ODBC information and click **Apply**
6. Restart all Modus services

In the users’ mail clients, a new :Quarantine folder will appear in the list along with a Spam subfolder.

Only messages trapped as spam will appear in the Spam subfolder (i.e. viruses or FAs won't be listed). The contents of the Spam folder should synchronize with what's visible in WebQuarantine.

## **Monitoring Database**

If you were using the PostgreSQL monitoring database from Modus version 4.2, but wish to convert this to an MSSQL database, we can give you a script that you can run to do this. However, **YOU WILL LOSE** any historical data that you had in your PostgreSQL database. If you want to convert the database to MSSQL, we recommend that you make a backup of your PostgreSQL database first.

## **PostgreSQL Monitoring**

If you were previously not running the monitoring database, or were running it in Access or MSSQL and want to change to PostgreSQL (but **DO NOT NEED** your historical data), please follow these instructions:

1. Go to ...Vircom\ModusProduct\DBStructures\PostgreSQL\Monitoring
2. Run the file ModusSQL.bat
3. Open the Modus console and go to **System > Monitoring Database** and enter your information in the “Native Postgres Database” section.
4. Click **Apply**
5. Restart all Modus services

This will create a database called Modus on the local server with the tables and procedures in it.

For instructions about what to do if you:

- Need to install the PostgreSQL Monitoring DB manually
- Already have the most recent version of PostgreSQL installed
- Already have an older version of PostgreSQL installed
- Want to install PostgreSQL remotely

Please refer to the Administration Manual.

## MSSQL Monitoring

1. Open MSSQL Enterprise Manager
2. Create the database or use an existing one
3. Go to ...Vircom\ModusProduct\DBStructures\SQL Server\Monitoring
4. Run the file CreateMonitoringSQL.exe and enter the following options
  - a. Server
  - b. Database
  - c. Username
  - d. Password
5. Create the ODBC connection
6. Open the Modus console and go to **System > Monitoring Database**
7. Enter your ODBC information
8. Click **Apply**
9. Restart all Modus services

## Extended Database

*NOTE: the extended database option is ONLY available to Modus Gate blockade customers (ie, those with more than one Modus server).*

We have optimized the extended database format for better performance and better cluster integration.

## MSSQL Extended database

1. Open MSSQL Enterprise Manager
2. Create the database or use an existing one
3. Open MSSQL Query Analyzer
4. Go to ...Vircom\ModusProduct\DBStructures\SQL Server\ExtendedDB
  - a. If this is a new extended database (you haven't used the extended database before), run the script mssql\_extendeddb\_new.sql
  - b. If you already have an extended database, but are updating the format for our new features, run the script mssql\_extendeddb\_upgrade.sql
5. Migrate the mailbox settings from the registry to the database using the SyncUserRegDB.exe tool
  - a. If you are creating a brand new extended database, make sure you select the option "**convert existing registry mailboxes**" (this option is NOT selected by default)

OR

- b. If you are upgrading an existing extended database, make sure you select the option “**synchronize existing database mailboxes**” (this option is selected by default)
6. If this is a new Extended database for you (you did not use it previously), create an ODBC connection
7. Open the Modus console and go to **Auth > ODBC Database** and make sure the **Use Extended Database** option is checked.
8. Enter your ODBC information and click **Apply**
9. Restart all Modus services

*NOTE: you MUST complete these steps in order – you cannot perform step 5 before running the scripts in step 4. If you need to rollback, you must then move the mailbox settings from the database back to the registry, please contact Vircom.*

### **SieveStore Database**

*Please note – this section is for brand new installs of Modus only. Anyone with existing SieveStore databases should not make any changes to their databases until Modus version 4.4.*

### **MSSQL SieveStore Database (New Installs ONLY)**

1. Open MSSQL Enterprise Manager
2. Create the database or use an existing one
3. Open MSSQL Query Analyzer
4. Go to ...Vircom\ModusProduct\DBStructures\SQL Server\SieveStore
5. Run the script mssql\_sievestore\_new.sql
6. Create the ODBC connection
7. Open the Modus console and go to **Anti-Spam > Sieve Database**
8. Enter your ODBC information and click **Apply**
9. Restart all Modus services

***Blacklist/Whitelist import tool available***

We have a command line tool you can use to import blacklists or whitelists.

1. Go to C:\program files\Vircom\ModusGate
2. Open the file **blacklistimport.exe**

## WebQuarantine 4.2/4.3 Interface Redesign

Modus WebQuarantine 4.3 performs super-fast for dial-up users. Its striking but simple interface is intuitive and has been designed with browser compatibility in mind. It supports Safari (Mac OSX) and Opera 8, as well as Firefox 1.0 and later, Netscape 7.1 and later, and IE 5.5 and later (for PC only – we can't support IE for Mac because of its limitation with multiple style sheets. Unfortunately if we try to support IE for Mac, it restricts us from being able to support other browsers).

### **New features**

#### **Quarantine Search**

Quarantine search ability is now available. The search feature scans these attributes of a message only:

- Subject
- From
- To
- Cc

From any of the folder views, enter your search criteria and click the magnifying glass.

#### **Resizable text and 800X600 support**

WebQuarantine's fast-loading, slick interface has just been made even better – it now scales to fit your resolution (previously was optimized for 1024X768) and supports resizable text.

To resize your text, set the font size you want to use directly in your browser (for example, got to **View > Text Size** in either Internet Explorer or Firefox to set a new text size).

#### **Message headers**

You can now view message header details in WebQuarantine!

Click **Full Header** in a message window, and the header detail will be displayed.

Click **Partial Header**, and only the basic header information will be displayed.

#### **Persist Sorting Order**

It is now possible for users to have their preferred list sorting order persisted between web sessions. If this feature is enabled, when the user makes a change to the list sorting order, WebQuarantine will remember the change and persist it for future web sessions.

*NOTE: this feature affects the performance speed of WebQuarantine. It is disabled by default for the reason that when users login, their inbox will take a while to load because the server must re-order their messages according to any sorting preferences they made during their last web session.*

1. Go to /Program Files/Vircom/web/webquarantine
2. Open the WebMailSvr.ini file
3. Add the following line under [Default:Settings]:  
PersistSort=1

#### 4. Save the file

You can turn off this feature by setting the line to equal 0.

### **Mailbox statistics**

Users can find out graphical information about their email traffic from the Statistics section. This section provides statistical breakdowns where users can choose to view:

- a histogram of daily, weekly, monthly or the last twelve months of statistics about the amount of legitimate email vs the amount of spam, or email with forbidden attachments or viruses in them that have been received by their mailbox.
- a daily, weekly, monthly, or 12-month comparison of the different types of spam received.

### **Foreign Language Support**

The following languages are available selections for the interface from the login screen: English, French, German, Spanish, Norwegian, Danish, Dutch, Swedish, Italian and Turkish.

### **Domain customization**

You can create a custom look for your WebQuarantine for each of your domains.

Please refer to the customization instructions at the end of this document for specific information about how to do this.

### ***WebQuarantine Known Issue***

The date displayed in the message list is the date when the message was sent (the timestamp given to the message by the sender's mail client) and not when it was received (by the receiving server).

## WebQuarantine 4.3 Interface Customization

For Modus version 4.3, we are still including the older 4.1 WebQuarantine interface – these files are contained in the \Program Files\Vircom\Web\WebMail\WebSite directory.

However, the following customization instructions pertain specifically to the new 4.2/4.3 WebQuarantine application, contained in the \Program Files\Vircom\Web\WebMail\WebRoot directory. Please contact Vircom if you require the customization instructions for the 4.1 WebQuarantine application.

There are many levels of customization that you can do to the web interface, depending on how far you want to take your customization:

- you can substitute your company logo for the Vircom logos (which appear on the login and on each web page)
- you can modify attributes of the Vircom theme such as the color or the size of the text
- you can bypass Vircom's login page and have your users access their WebQuarantine through your own portal
- you can create a completely different theme for the web interface that bears no resemblance to the Vircom theme – this theme will not be overwritten by future upgrades, BUT any interface enhancements made by Vircom will not be reflected in your custom-built interface. We provide only very basic customization information here – enough that if you know what you're doing, you'll know how to support your own customizations and you can go ahead and build your own interface.

*Note: The web.config and style.css files contain the product default values. Never alter these files because any work you do be lost upon upgrading the software. Change the custom.config instead. A Modus upgrade will not overwrite your files – these files will be untouched and your interface changes will not be affected. Please note also that Vircom Technical support cannot debug any custom interfaces you build. We can support only basic style changes to the Vircom interface that include rebranding and recoloring (changing images and modifying CSS styles).*

### Browser Compatibility for WebQuarantine

Webmail supports Safari (Mac OSX) and Opera 8, as well as Firefox 1.0 and later, Netscape 7.1 and later, and IE 5.5 and later.

### Custom.Config Basic Functionality Customization

*NOTE: Any modifications you make in the custom.config file will require you to perform an IIS reset after you have finished.*

1. The default language of the WebQuarantine interface is defined in this key. The value must match an existing folder under *Locales*.  
<add key="DefaultLanguage" value="en"></add>
2. The default theme of the WebQuarantine interface is defined in this key. The value must match an existing theme folder under *Themes*.  
<add key="DefaultTheme" value="vircom"></add>

3. This is the domain name or IP address of your Webmail Server service.  
<add key="WebMailServerAddress" value="localhost"></add>
4. This is the port number of your WebMail Server service.  
<add key="WebMailServerPort" value="31804"></add>
5. This is the character set in which the page will be displayed.  
<add key="Charset" value="iso-8859-1"></add>
6. This is the path of the temporary folder that the installation program configures automatically.  
<add key="Temp" value=""></add>
7. This is the path of the log folder that the installation program configures automatically.  
<add key="LogDir" value=""></add>
8. This is the relative path and file name of the Login page. If you want to design your own login page or you want to integrate WebQuarantine with your portal, change this value to your to the relative path and file name of your custom-designed login page. When logging off, users will be redirected to this page instead of the main WebQuarantine login page.  
<add key="LoginPage" value="Login.aspx"></add>
9. This is the name of the application that will be shown in the browser windows title bar.  
<add key="Title" value="Webmail"></add>
10. This option determines whether WebQuarantine should parse messages to find out if there is an attachment.  
<add key="ShowPaperClip" value="false"></add>  
*NOTE: When this option is turned on, you might encounter performance drops for POP3 accounts since the message must be downloaded completely. This does not affect IMAP4 accounts.*  
Set the value to "true" to enable or to "false" to disable it.
11. To show ONLY those settings that users can modify (and therefore hide anything that's been set at the system or domain level to override user preferences), change the following key to "false".  
<add key="SettingsAccessVisible" value="true"></add>

## Logos

In the custom.config file, you can set the image and hyperlink for the Login logo and the top menu logo. These images must exist in your selected theme in order to work.

```
<add key="LoginLogoUrl" value="http://www.vircom.com">  
<add key="LoginLogoImage" value="LogoLogin.gif"></add>
```

```
<add key="MenuLogoUrl" value="http://www.vircom.com">  
<add key="MenuLogoImage" value="LogoMenu.gif"></add>
```

### **Custom Login page or Portal Integration**

You can create your own login page or insert the login form in your portal. Your login page should include a form with the two following form fields:

```
<input type="text" name="txtLogin"/>  
<input type="password" name="txtPassword"/>
```

The page's form action should be set to "Login.aspx" and the method set to "POST". Here's a simple Login page:

```
<html>  
<body>  
<form action="Login.aspx" method="POST">  
<input type="text" name="txtLogin"/>  
<input type="password" name="txtPassword"/>  
<input type="submit" value="Login"/>  
</form>  
</body>  
</html>
```

### **Theme Customization**

The WebQuarantine application theme is made through a main CSS file (and if you vary functionality between domains, you'll also need a customized .config file). DO NOT alter the Style.css file or the Web.config file (or you will lose all your work when you perform a Modus upgrade). Instead, you must redefine colors, fonts, and other attributes in the Custom.CSS, and any functionality variations (see config file attributes above) in the custom.config files.

Any changes you make to the custom files will override the values in the style.css and web.config files.

For domain customization, create css and config files and name them according to the domain, for example:

domain.com.css (which should be saved in your custom theme directory)

domain.com.config (which should be saved in the webroot directory)

domain.net.css (which should be saved in your custom theme directory)

domain.net.config (which should be saved in the webroot directory)

These domain files will override the custom.css and custom.config files which override the main style.css and web.config files.

*NOTE: you only have to create a domain customized config file if you want to vary functionality between domains as well as the look and feel of it. Otherwise only create a domain customized CSS file for your theme.*

### Changing the Login page color:

The login page orange color constitutes of an image (Login\_RoundBorder.gif) and a table cell. For example, to change the color to lightgrey:

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following line:

```
#tdLoginRight
{
background-color: lightgrey;
}
```
4. Save and close the file

*Note that unless you change the Login\_RoundBorder.gif image to lightgrey, it will look odd, so you can edit that file in an image editor or you can hide it altogether. To do so, add the following lines in the custom.css right after the lines previously added:*

```
#tdLoginMiddle
{
display: none;
}
```

### Changing the Top Menu color:

The top menu constitutes of an image (LogoMenu.gif) which is configured in the custom.config file, and a gradient image of 1 pixel width. The gradient image adds a level of depth to the menu bar while preserving a very small file size. If you want to change the gradient coloring, open the GradientMenu.gif file in an image editor such as Gimp, PaintShopPro or Photoshop and change the color or gradient value of the image to your preference. You can also discard the gradient in the top menu and only use a solid color, such as lightgrey. To do this:

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following line:

```
.Menu
{
background-color: lightgrey;
}
```

4. Save the file

### Changing the lists hover color:

Each message status has a separate class. This allows you to define different attributes for when an email is read, unread or deleted. In order to change the hover color, you will need to change each of these classes:

1. Go to the Themes\Vircom folder

2. Open the custom.css file
3. Add the following line:

```
.dgListItemHover  
{  
background-color: lightgrey;  
}
```

```
.dgListItemUnreadHover  
{  
background-color: lightgrey;  
}
```

```
.dgListItemDeletedHover  
{  
background-color: lightgrey;  
}
```

4. Save the file

### **Changing the background color of all panels:**

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following lines:

```
.MessageViewMsgHeader,  
.SettingsAccount,  
.SettingsOption,  
.SettingsOptionGeneral,  
.SettingsFolders,  
.SettingsOptionsAntiSpam,  
.SettingsOptionsAntiVirus,  
.SettingsOptionsRules,  
.SettingsOptionsAutoReply,  
.SettingsContacts,  
.SettingsOptionsHome,  
.SettingsOptionsBusiness,  
.SettingsTrusted,  
.SettingsBlocked,  
.SettingsOptionsBlocked,  
.SettingsOptionsTrusted,  
.SettingsAliases,  
.SettingsOptionsReporting,  
#divContactEditor_main,  
.DiagnosticContainer  
{
```

```
background-color: lightgrey;
}
```

4. Save the file

### Removing Statistics (or other major menu items)

If you are not using the monitoring service, or if you prefer users not to have access to their mail statistics, you can remove the Statistics menu option from the web interface.

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following line:

```
#tdStatistics
{
display: none;
}
```

4. Save the file

*NOTE: these instructions apply to the other menu items: #tdAddressBook, #tdFolders, #tdSettings, #tdLogoff. Change the syntax for the line in step 3 from <#tdStatistics> to the menu item you want to hide.*

### Hiding a section of the settings:

As with the login page, it is possible to hide certain parts of the page. This is especially useful if you don't want your users to access particular types of settings.

#### To hide the options section:

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following line:

```
#SettingsOptions
{
display: none;
}
```

4. Save the file

#### To hide the email filtering section:

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following line:

```
#SettingsFiltering
{
```

```
display: none;
}
```

4. Save the file

**To hide the user contact information section:**

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following line:

```
#SettingsUserInfo
{
display: none;
}
```

4. Save the file

**To hide the rules section:**

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following line:

```
#SettingsRules
{
display: none;
}
```

4. Save the file

**To hide the auto-reply section:**

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following line:

```
#SettingsAutoreply
{
display: none;
}
```

4. Save the file

**To hide the external accounts section:**

1. Go to the Themes\Vircom folder
2. Open the custom.css file

3. Add the following line:

```
#SettingsAccounts
{
display: none;
}
```

4. Save the file

**To hide the aliases section:**

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following line:

```
#SettingsAliases
{
display: none;
}
```

4. Save the file

**To hide the Server Blocked/Trusted list from the Settings page:**

1. Go to the Themes\Vircom folder
2. Open the custom.css file
3. Add the following line:

```
#TableRowWhitelistServerTitle,
#TableRowWhitelistServerData,
#TableRowBlacklistServerTitle,
#TableRowBlacklistServerData
{
display:none;
}
```

4. Save the file

### **WebQuarantine Message Customization**

You can customize your own WebQuarantine messages (what we call “strings”) – this could be especially useful for foreign language support if the translation provided does not adequately communicate an action or system response.

Each language has its own strings file stored in:

```
\Program Files\Vircom\Web\Quarantine\WebRoot\Locales
```

There is a strings.xml file – the default translations provided with WebQuarantine – and a custom.xml file. Make your changes in the custom.xml file (as follows in the instructions below) and this file will override strings.xml.

### **Changing default strings**

1. Go to the language folder whose messages you want to customize and open both the strings.xml and the custom.xml files
2. Copy and paste the strings to be customized from the strings.xml file into the custom.xml file
3. Modify the strings in the custom.xml file and save it.
4. You can also include HTML formatting instructions in the custom.xml file to specify how you want the customized strings to be displayed. This is useful, for instance, for the TEXT1000 & TEXT1001 tags which are shown at the top and bottom of the right-hand side of the login page respectively (where the beta version information and the upcoming features information was previously displayed).
5. Save the strings.xml file as well to change its timestamp so that the changes you have made can be viewed immediately (not changing the timestamp on the strings.xml file will mean that the customized strings are not shown until you restart IIS).

## Bug Fixes

- #2624 Fixed: Extended DB fallback DSN wasn't going back to original source when it came back up.
- #2851 Fixed: Stability issue with Moduscan/Modusadm if ODBC connection dropped to Quarantine or Sievestore
- #2902 Fixed: Installer would stop all modus services even if installing only web components.
- #2991 Fixed: Problem with SPF with certain forms of MAILFROM: in SMTP Transaction.
- #2994 Fixed: Blacklist behavior of "delete" was not always applied, messages were still getting quarantined.
- #3014 Fixed: Erroneous service "died" warnings in event viewer and at startup in windows 2003.
- #3019 Fixed: Problem with mime-encoded messages where the result was that the sub-parts became attachments.
- #3021 Fixed: Problem where manually blacklisted messages caught in quarantine were "reportable" as false-positives.
- #3023 Fixed: Problem with release from webquarantine when from: and to: matched the Email address of mailbox owner.
- #3040 Fixed: Quarantine report had a bug whereas 1st character of subject was truncated.
- #3044 Fixed: Queue Delivery Level statistic was stuck at an arbitrary value.
- #3092 Fixed: Reverse DNS lookup was functioning even if you disabled it in the console.
- #3121 Fixed: Erroneous message was displayed when users tried to report a virus from "Quarantine"
- #3135 Fixed: Quarantine reports were not generating properly with custom and original templates.
- #3216 Fixed: Sieve engine was having problems with messages containing base64 encoding with malformed headers.
- #3221 Fixed: Routing issue if multiple routes going to same source and primary is down while set to "accept all".
- #3302 Fixed: dual virus engine problem when changing the scanning order.
- #3050 Improved: SMTPDS Delivery strategy when falling back to secondary MX records.
- #3241 Improved: SMTPDS Delivery strategy when destination host closes the connection, we fallback to secondary MX record.
- #3179 Improved: Error handling when adding new email address to blocked/trusted senders in quarantine report.
- #2945 Added: Feature that allows customers to have administrator review one-click release requests.
- #2961 Added: Tool tips for the default quarantine report.
- #3030 Added: Panel in SMTPDS configuration to select an IP instead of a generic text box, preventing the addition of bad IPs.
- #3068 Added: Auto-cleanup support for "Category 12" entries in the quarantine (scanning errors).
- #3143 Added: Link under quarantine to select multiple categories.
- #3209 Added: Exchange routing information (authentication server) in the route wizard.
- #2934 Removed: Antivirus options in Webadmin if running modusgate with antispam-only.

- #3075 Removed: In Domains-> Blacklist Tab & Users->Blacklist Tab: user shouldn't be able to edit the "Send to recipient with tag" option
- #3119 Changed: renamed blacklist "blocked list" to "blocked senders" and whitelist "safe list" to "trusted senders" in webadmin.
- #3142 Changed: resized the pie chart in webmonitor and statistics section of the webmail.

### **Known Issues**

- PostgreSQL is not upgraded a during Modus upgrade (the latest version is only installed if customer is installing PostgreSQL for the first time). A batch file for PostgreSQL 8.0.6 is installed with a Modus upgrade and can be run separately. You will find the file in product folder with a readme instruction file
- #3147 Some emails will still be quarantined although their sender is in a user's trusted sender list. This behavior comes from one of the following causes:
  - The message has been generated from a mailing list
  - The original recipient has some forward to setting in their preferencesDetailed description:  
A message has been received from a trusted sender and was not scanned. SMTPDS forwards this message to ModuScan again and then ModuScan does not recognize this message as from trusted source.
- #3307-8 System Health beta issues: average counters are not always as accurate as they should be because of counter fluctuations.
- #3397 The stop command in Sieve doesn't unconditionally stop the scanning